Tivoli Public Key Infrastructure

Systemverwaltung

Version 3 Release 7.1

SH12-2979-02

Tivoli Public Key Infrastructure

Systemverwaltung

Version 3 Release 7.1

SH12-2979-02

Copyrightvermerke

Copyright © 1999, 2001 IBM Corp., einschließlich dieser Dokumentation und aller Software. Alle Rechte vorbehalten. Kann nur gemäß der Softwarelizenzvereinbarung von Tivoli Systems bzw. IBM oder dem Anhang für Tivoli-Produkte der IBM Nutzungsbedingungen verwendet werden. Diese Veröffentlichung darf ohne vorherige schriftliche Genehmigung der IBM Corp. weder ganz noch in Auszügen auf irgendeine Weise - elektronisch, mechanisch, magnetisch, optisch, chemisch, manuell u. a. - vervielfältigt, übertragen, aufgezeichnet, auf einem Abrufsystem gespeichert oder in eine andere Computersprache übersetzt werden. Die IBM Corp. gestattet Ihnen in begrenztem Umfang, eine Hardcopy oder eine Reproduktion einer maschinenlesbaren Dokumentation für den eigenen Gebrauch zu erstellen, unter der Voraussetzung, dass jede dieser Reproduktionen mit dem Copyrightvermerk der IBM Corp. versehen ist. Weitere das Copyright betreffende Rechte werden nur nach vorheriger schriftlicher Genehmigung durch die IBM Corp. gewährt. Die Veröffentlichung dient nicht zu Produktionszwecken. **Die in diesem Dokument aufgeführten Beispiele sollen lediglich zur Veranschaulichung und zu keinem anderen Zweck dienen.**

Marken

AIX, DB2, DB2 Universal Database, IBM, RS/6000, SecureWay, Tivoli and WebSphere sind in gewissen Ländern eingetragene Marken der International Business Machines Corp. oder von Tivoli Systems Inc.

Das Programm Tivoli PKI (im folgenden als ″Programm″ bezeichnet) enthält Komponenten von IBM WebSphere Application Server und IBM HTTP Web Server (″IBM Server″). Diese dürfen nur zusammen mit dem Programm installiert und entsprechend der für das Programm geltenden Lizenzvereinbarungen in Kombination mit diesem verwendet werden. Die IBM Server müssen auf derselben Maschine wie das Programm installiert sein. Sie sind nicht berechtigt, sie unabhängig vom Programm zu installieren und zu verwenden.

Das Programm Tivoli PKI (im folgenden als ″Programm″ bezeichnet) enthält Komponenten von DB2 Universal Database. Diese Komponenten dürfen nur zusammen mit dem Programm installiert und entsprechend der für das Programm geltenden Lizenzvereinbarungen in Kombination mit diesem verwendet werden, um Daten zu speichern und zu verwalten, die vom Programm verwendet oder generiert werden. Für andere Datenverwaltungsoperationen ist der Einsatz nicht gestattet. Diese Lizenz gilt z. B. nicht für eingehende Verbindungen zur Datenbank, die von anderen Anwendungen aus für Abfragen und Berichtserstellungsoperationen hergestellt werden. Sie sind lediglich zur Installation und Verwendung dieser Komponenten auf der gleichen Maschine berechtigt, auf der auch das Programm installiert und verwendet wird.

Das Programm enthält Komponenten des IBM WebSphere Application Server und des IBM HTTP Web Server (″IBM Server″). Sie sind nicht berechtigt, die IBM Server zu anderen Zwecken als in Verbindung mit der lizenzgerechten Verwendung des Programms zu benutzen. Die IBM Server müssen auf derselben Maschine wie das Programm installiert sein. Sie sind nicht berechtigt, sie unabhängig vom Programm zu installieren und zu verwenden.

Java und alle auf Java basierenden Marken und Logos sind in gewissen Ländern Marken der Sun Microsystems, Inc.

Microsoft, Windows, Windows NT und das Windows-Logo sind in gewissen Ländern Marken der Microsoft Corporation.

UNIX ist eine eingetragene Marke und wird ausschließlich von der X/Open Company Limited lizenziert.

Pentium ist in gewissen Ländern eine Marke der Intel Corporation.

Bemerkungen

Die vorliegenden Informationen wurden für Produkte und Services entwickelt, die auf dem deutschen Markt angeboten werden. Möglicherweise bietet IBM die in dieser Dokumentation beschriebenen Produkte, Services oder Funktionen in anderen Ländern nicht an. Informationen über die gegenwärtig im jeweiligen Land verfügbaren Produkte und Services sind beim IBM Ansprechpartner erhältlich. Hinweise auf IBM Lizenzprogramme oder andere IBM Produkte bedeuten nicht, daß nur Programme, Produkte oder Dienstleistungen von IBM verwendet werden können. Anstelle der IBM Produkte, Programme oder Dienstleistungen können auch andere ihnen äquivalente Produkte, Programme oder Dienstleistungen verwendet werden, solange diese keine gewerblichen Schutzrechte der IBM verletzen. Die Verantwortung für den Betrieb der Produkte, Programme und Dienstleistungen in Verbindung mit Fremdprodukten liegt beim Kunden, soweit solche Verbindungen nicht ausdrücklich von IBM bestätigt sind.

Für in diesem Handbuch beschriebene Erzeugnisse und Verfahren kann es IBM Patente oder Patentanmeldungen geben. Mit der Auslieferung dieses Handbuchs ist keine Lizenzierung dieser Patente verbunden. Lizenzanforderungen sind schriftlich an IBM Europe, Director of Licensing, 92066 Paris La Defense Cedex, France, zu richten. Anfragen an obige Adresse müssen auf englisch formuliert werden.

Dieses Programm enthält Sicherheitssoftware von RSA Data Security, Inc. Copyright © 1994 RSA Data Security, Inc. Alle Rechte vorbehalten.

Dieses Programm enthält STL-Software (STL = Standard Template Library) von Hewlett-Packard Company. Copyright (c) 1994.

- Die Berechtigung zum Verwenden, Kopieren, Ändern, Verteilen und Verkaufen dieser Software sowie der zugehörigen Dokumentation für die gewünschten Zwecke wird hiermit gebührenfrei erteilt. Voraussetzung hierfür ist allerdings, daß der o. a. Copyrightvermerk auf allen Kopien erscheint, und daß sowohl dieser Copyrightvermerk als auch dieser Berechtigungshinweis in der zugehörigen Dokumentation aufgeführt werden. Hewlett-Packard Company macht keine Angaben zur Eignung dieser Software für bestimmte Zwecke. Sie wird ohne Modifikationen und ohne Gewährleistung bereitgestellt.

Dieses Programm enthält STL-Software (STL = Standard Template Library) von Silicon Graphics Computer Systems, Inc. Copyright (c) 1996 - 1999.

- Die Berechtigung zum Verwenden, Kopieren, Ändern, Verteilen und Verkaufen dieser Software sowie der zugehörigen Dokumentation für die gewünschten Zwecke wird hiermit gebührenfrei erteilt. Voraussetzung hierfür ist allerdings, daß der o. a. Copyrightvermerk auf allen Kopien erscheint, und daß sowohl dieser Copyrightvermerk als auch dieser Berechtigungshinweis in der zugehörigen Dokumentation aufgeführt werden. Silicon Graphics macht keine Angaben zur Eignung dieser Software für bestimmte Zwecke. Sie wird ohne Modifikationen und ohne Gewährleistung bereitgestellt.

Andere Namen von Unternehmen, Produkten oder Dienstleistungen können Marken oder Dienstleistungsmarken anderer Unternehmen sein.

Inhaltsverzeichnis

Tabellen ix

Vorwort xi

Zielgruppe xi

Bezugsinformationen xi

Inhalt des Handbuchs xii

In diesem Handbuch verwendete Konventionen xiii

Kundenunterstützung xiii

Informationen zu Tivoli PKI im Web xiii

Kapitel 1. Informationen zu Tivoli PKI 1

Kapitel 2. Übersicht 3

Kapitel 3. Informationen zur Vorgehensweise 5

Tivoli PKI verwalten 5

Befehle unter Windows NT eingeben 5

Tivoli PKI-Kennwörter ändern 5

Serverkomponenten starten und stoppen 8

Tivoli PKI-IP-Adressen ändern 10

System sichern und wiederherstellen 10

Anzahl von Benutzern und Zertifikaten überwachen 11

Zertifikataktivität überwachen 12

WebSphere Application Server verwalten 14

Status des WebSphere Application Server prüfen 14

WebSphere Application Server-Protokolle prüfen 15

HTTP Server verwalten 15

Status des HTTP Server prüfen 16

HTTP Server-Protokolle prüfen 17

CA-Server verwalten 17

Listener-Port des CA-Servers ändern 18

CA-Sendeaufrufintervall ändern 18

CRL-Einstellungen ändern 19

ICL-Schutzregel ändern 20

ICL-Schutzschlüssel ändern 20

Integrität der CA-Serverdatenbank prüfen 21

CA-Zertifikat über gegenseitige Zertifizierung anfordern 22

CA-Zertifikat mit Hilfe des Hierarchiemodells anfordern 25

CA-Zertifikat von Fremd-CA erhalten 28
Aktualisierungen nach Änderung der CA-Hierarchie vornehmen 29
Schlüsselbund des Webservers nach Aufbau der CA-Hierarchie aktualisieren 29
CA-Schlüssel aktualisieren 30
CA-Serverprotokolle prüfen 34
CA-Serverstatus prüfen 34
CRL-Verteilungspunkte aktivieren 35
RA-Server verwalten 35
Registratoren hinzufügen 36
Verschlüsselung für die RA-Datenbank aktivieren 39
RA-Server-Listener-Port ändern 40
RA-Sendeaufrufintervall ändern 40
RA-Wiederholungsintervall ändern 41
RA-Serverprotokolle prüfen 41
RA-Serverstatus prüfen 41
RA-Einstellungen für die Kommunikation mit dem Directory ändern 42
Übergabe der Trust-Kette aktivieren bzw. inaktivieren 43
Mehrere RAs installieren 44
Prüfsubsystem verwalten 46
Protokolleinträge anzeigen 47
Protokolleinträge suchen 49
Prüfserver-Port auf dem Prüf-Client ändern 49
Sendeart für Ereignisse vom Prüf-Client ändern 49
Listener-Port für den Prüfserver ändern 51
Anzahl der Bindungsversuche zwischen Prüfserver und Prüf-Client ändern 51
Intervall zwischen Bindungsversuchen ändern 51
Protokolleinstellungen ändern 52
Prüfberichte generieren 54
Prüfprotokolldateien archivieren und unterzeichnen 55
Integrität der Datenbank des Prüfservers und der Archivierungsdateien prüfen 55
Status des Prüfservers prüfen 58
Prüfserverprotokolle prüfen 59
DB2-Datenbanken verwalten 60
Status der DB2-Datenbanken prüfen 60
DB2-Protokolle prüfen 62
Directory-Server verwalten 62
Status des Directory-Servers prüfen 63
Directory-Server-Protokolle prüfen 64
IBM SecureWay 4758 PCI Cryptographic Coprocessor verwalten 64

Kapitel 4. Erläuterungen 65

Tivoli PKI - Sicherheit 65
Zugriffssteuerungsliste (Access Control List - ACL) 65
Zertifikatsaussteller (Certification Authority - CA) 66
CA-Hierarchien 66
Zertifikatserweiterungen 67
Zertifikatswiderrufsliste (CRL) 70
Gegenseitige Zertifizierung 70
Zertifizierung 71
Digitale Zertifikate 71
Registrierte Namen 71
Liste der ausgestellten Zertifikate (ICL) 71
Unterzeichnen und Gültigkeitsprüfung für Unterschriften 72
Registrierungsstellen (RA) 72
Registratoren 72
Registrierungsdomänen 73
Mehrere RAs 73
Übergabe der Trust-Kette 73
IBM SecureWay 4758 PCI Cryptographic Coprocessor 73
Unterschiede zwischen den Optionen für Beibehaltung und Nicht-Beibehaltung 74
Aufgabenbereiche und Profile 76
IBM 4758 Cryptographic Coprocessor in der Tivoli PKI-Umgebung installieren und klonen 76
Prüfung 77
Protokolleinträge 78
Prüfereignisse 78
Masken für Prüfereignisse 78
Verbindliche und optionale Prüfereignisse 78
Integritätsprüfung 79
Integritätsversiegelung 79
Prüfprotokoll archivieren 79
DB2 Datenbanken 79
Webserver 79
IBM WebSphere Application Server 80
IBM HTTP Server 80
IP-Aliasing 80
Directory-Server 81
Objektkennungen 81

Kapitel 5. Referenzinformationen 83

Konfigurationsdateien 83
Dateibeschreibung 85
Konfigurationsdatei für CA-Server 85
Konfigurationsdatei für RA-Server 95
Konfigurationsdatei für Prüfserver 105
Konfigurationsdatei für Prüf-Client 109
Befehlszeilendienstprogramme 112
Dienstprogramm CA Certification 112
Dienstprogramm Add RA User 115
Dienstprogramm Enable RA Database Encryption 115
Dienstprogramm Audit Archive and Sign 116
Dienstprogramm Audit Integrity Check 116
Dienstprogramm Create New RA 117
Dienstprogramm Multiple RA Enrollment Authorization 118
| Dienstprogramm Bulk Certificate Issuance 118
| Dienstprogramm CA Key Update 124
Felder für Prüfereignisse 125
Prüfereignisse 126
Prüfung von Datenbankdaten 129
Schlüsseltabelle 129
Tabelle für Ereignisbewertung 130
Tabelle zur Ereignissteuerung 130
Quellentabelle 131
Tabelle der berechtigten Entitäten 131
Tabelle der berechtigten Aufgabenbereiche 131
Tabelle der Arten betroffener Entitäten 132
Tabelle der Komponentenarten 132
Tabelle für Prüfprotokoll 132
Systemtabelle 134
Fehlerbehebung 135
Grundlegende Fehlerbehebung 135
Fehlerbehebung mit aktivierter Nachrichtenerstellung auf Debug-Stufe 135

Glossar 137

Index 157

Tabellen

1. WebSphere Application Server-Protokolle über Transaktionen mit dem Setup Wizard 15
2. IBM WebSphere Application Server - Protokolle über Transaktionen mit der Registrierungsanwendung 15
3. HTTP Server-Protokoll 17
4. Protokolle des CA-Servers 34
5. RA-Server-Protokolle 41
6. Spaltenbeschreibungen der Sichten für die Tivoli PKI-Prüfdatenbank 47
7. Protokolle des Prüf-Servers 59
8. Datenbankpositionen 60
9. Protokolle des Directory-Servers 64
10. Zertifikatserweiterungen 67
11. Modell für IBM HTTP Server mit drei Servern und drei Ports 80
12. Tivoli PKI-Konfigurationsdateien 84
13. CA-Server - Konfigurationsdatei 86
14. RA-Server - Konfigurationsdatei 96
15. Prüf-Server - Konfigurationsdatei 106
16. Prüf-Client - Konfigurationsdatei 110
17. Rollover-Prozess für CA-Schlüssel 124
18. Felder für Prüfereignisse 125
19. Prüfereignisse 126
20. Felder in der Schlüsseltabelle 129
21. Felder in der Tabelle für die Ereignisbewertung 130
22. Felder in der Tabelle für die Ereignissteuerung 130
23. Felder in der Quellentabelle 131
24. Felder in der Tabelle berechtigter Entitäten 131
25. Felder in der Tabelle berechtigter Aufgabenbereiche 131
26. Felder in der Tabelle der Arten betroffener Entitäten 132
27. Felder in der Tabelle der Komponentenarten 132
28. Felder in der Prüfprotokolltabelle 132
29. Felder in der Systemtabelle 134

Vorwort

Dieses Handbuch erläutert die Verwaltung des Tivoli PKI-Systems. Es beschreibt die Prozeduren zum Starten und Stoppen der Server, zum Ändern von Kennwörtern, zum Verwalten der Server-Komponenten sowie zum Ausführen von Prüfungen und Datenintegritätsüberprüfungen.

Das aktuelle Release des Produkts unterstützt ausschließlich AIX-Plattformen. Alle Angaben bezüglich Microsoft Windows sind zu ignorieren.

Zielgruppe

Dieses Buch bietet Task-orientierte Informationen, die Systemadministratoren für den Betrieb und die Verwaltung des Tivoli PKI-Systems benötigen.

Die Benutzer dieses Handbuchs sollten in den folgenden Bereichen über praktische Erfahrungen verfügen:

- Betriebssystem AIX oder UNIX
- Betriebssystem Windows NT
- Systemarchitektur
- Netzverwaltung
- Datenbankverwaltung
- Web-Server-Verwaltung
- Verzeichnisverwaltung

Bezugsinformationen

Die Produktdokumentation zu Tivoli PKI ist im PDF-Format (Portable Document Format) und im HTML-Format auf der Tivoli Website verfügbar. Zusammen mit dem Produkt werden die HTML-Versionen einiger Veröffentlichungen installiert; sie können über die Benutzerschnittstelle aufgerufen werden.

Bitte beachten Sie, dass seit der Erstellung der Dokumentation möglicherweise Änderungen am Produkt vorgenommen wurden. Aktuelle Produktinformationen sowie Informationen über den Zugriff auf Veröffentlichungen in der Sprache und im Format Ihrer Wahl finden Sie in den Release-Informationen. Die neueste Version der Release-Informationen ist auf der Website für Tivoli Public Key Infrastructure unter der folgenden Adresse verfügbar:

`http://www.tivoli.com/support`

Die Tivoli PKI-Bibliothek umfasst die folgende Dokumentation:

Einführung
: Dieses Handbuch enthält eine Produktübersicht, führt die Produktvoraussetzungen und Installationsverfahren auf und bietet Informationen zum Zugriff auf die verfügbare Online-Hilfe für jede Produktkomponente. Dieses Buch liegt in gedruckter Form vor und wird mit dem Produkt geliefert.

Systemverwaltung

Dieses Handbuch enthält Basisinformationen zur Verwaltung des Tivoli PKI-Systems. Es beschreibt die Prozeduren zum Starten und Stoppen der Server, zum Ändern von Kennwörtern, zum Verwalten der Server-Komponenten sowie zum Ausführen von Prüfungen und Datenintegritätsüberprüfungen.

Konfiguration

Dieses Handbuch enthält Informationen zur Verwendung des Setup Wizard für die Konfiguration eines Tivoli PKI-Systems. Sie können auf die HTML-Version dieses Handbuchs zugreifen, während Sie die Online-Hilfe des Wizards nutzen.

Registration Authority Desktop

Dieses Handbuch enthält Informationen zur Verwendung von RA Desktop für die Verwaltung von Zertifikaten während ihres Gültigkeitszeitraums. Sie können auf die HTML-Version dieses Handbuchs zugreifen, während Sie die Online-Hilfe des Desktops nutzen.

Benutzerhandbuch

Dieses Buch enthält Informationen über Abruf und Verwaltung von Zertifikaten. Es beschreibt, wie die Zertifikate mit den Browser-Registrierungsformularen von Tivoli PKI angefordert, erneuert und widerrufen werden. Außerdem erläutert es, wie eine Vorabregistrierung für PKIX-kompatible Zertifikate durchgeführt wird.

Anpassung

Dieses Buch beschreibt, wie die Tivoli PKI-Registrierungseinrichtung angepasst wird, um die Registrierung- und Zertifizierungsvorgaben im Rahmen Ihrer Unternehmensregeln zu unterstützen. Sie erfahren beispielsweise, wie HTML- und Java Server-Seiten, Mitteilungsschreiben, Zertifikatsprofile und Regel-Exits angepasst werden.

Inhalt des Handbuchs

Dieses Handbuch enthält die folgenden Informationen:

- Das Kapitel „Informationen zu Tivoli PKI" auf Seite 1 enthält eine kurze Beschreibung der Funktionen und des Leistungsspektrums von Tivoli PKI.
- Im Kapitel „Übersicht" auf Seite 3 wird erläutert, wie Sie dieses Handbuch bei der Verwaltung des Systems benutzen.
- Das Kapitel „Informationen zur Vorgehensweise" auf Seite 5 enthält Task-orientierte Informationen, mit deren Hilfe Sie Tivoli PKI und seine Komponenten verwalten und einsetzen können.
- Im Kapitel „Erläuterungen" auf Seite 65 werden die allgemeinen Konzepte beschrieben, die mit der Registrierung, der Zertifizierung und der Verwaltung in Zusammenhang stehen.
- Das Kapitel „Referenzinformationen" auf Seite 83 enthält Beschreibungen von Befehlszeilendienstprogrammen, Syntax und Parametern sowie Beschreibungen von Konfigurationsdateien und deren Inhalt. Außerdem finden Sie in diesem Kapitel Abschnitte zur Prüfung und zur Fehlerbehebung.
- Das Kapitel „Glossar" auf Seite 137 definiert die in diesem Handbuch verwendeten und möglicherweise neuen oder unbekannten Begriffe und Abkürzungen, die von Bedeutung sind.

In diesem Handbuch verwendete Konventionen

Besondere Begriffe und Aktionen werden in diesem Handbuch durch die Verwendung unterschiedlicher Schriftbildkonventionen hervorgehoben. Die Konventionen haben die folgende Bedeutung:

Konvention	Bedeutung
Fett	Befehle, Schlüsselwörter, Markierungen und andere Informationen, die exakt in der im Handbuch angegebenen Schreibweise verwendet werden müssen, werden durch **Fettdruck** kenntlich gemacht.
Kursiv	Variablen, die von Ihnen angegeben werden müssen, sowie neue Begriffe werden in *Kursivdruck* dargestellt. Diese Darstellungsweise wird außerdem zum Hervorheben von Begriffen und Ausdrücken verwendet.
`Monospace-Schrift`	`Monospace-Schrift` wird für Codebeispiele, Ausgabedaten und Systemnachrichten verwendet.

Kundenunterstützung

Wenn bei der Verwendung eines Tivoli Produkts Probleme auftreten, können Sie über die Adresse **http://www.support.tivoli.com** die Homepage der Tivoli Unterstützung aufrufen. Nachdem Sie über diese Seite das Formular für die Kundenregistrierung aufgerufen und übergeben haben, stehen Ihnen im Web zahlreiche Services für die Kundenunterstützung zur Verfügung.

Kunden in Deutschland, Österreich oder der Schweiz können eine der folgenden Telefonnummern anrufen:

- Deutschland: **01805-00-1242**
- Österreich: **01-1706-6000**
- Schweiz: **0800-555454**

Ihre Erfahrungen bei der Verwendung von Tivoli-Produkten und -Dokumentationen interessieren uns ebenso wie Verbesserungsvorschläge. Wenn Sie Anmerkungen oder Anregungen hinsichtlich dieser Dokumentation machen möchten, senden Sie bitte eine E-Mail an pubs@tivoli.com.

Informationen zu Tivoli PKI im Web

Kunden von Tivoli und IBM Tivoli können für alle Sicherheitsprodukte von Tivoli und zu Tivoli PKI Onlineinformationen erhalten.

Wichtige Angaben zu den aktuellsten Produktaktualisierungen und Serviceinformationen für Tivoli PKI finden Sie auf der folgenden Website:
http://www.tivoli.com/support/secure_download_bridge.html

Informationen zum Produkt 'Tivoli Public Key Infrastructure' finden Sie auf der folgenden Website: **http://www.tivoli.com/products/index/secureway_public_key/**

Informationen zu anderen Tivoli Produkten für die Sicherheitsverwaltung finden Sie im Web unter der folgenden Position: **http://www.tivoli.com/products/solutions/security/**

1

Informationen zu Tivoli PKI

Dank Tivoli Public Key Infrastructure (Tivoli PKI) wird die Authentifizierung von Benutzern und die Bereitstellung von gesicherter Kommunikation durch Anwendungen möglich:

- Unternehmen können digitale Zertifikate in Übereinstimmung mit ihren Registrierungs- und Zertifizierungsrichtlinien ausstellen, publizieren und verwalten.
- Unterstützung für PKIX- (Public Key Infrastructure for X.509 Version 3) und CDSA-Verschlüsselungsstandards (CDSA = Common Data Security Architecture) zur Realisierung der Interoperabilität zwischen verschiedenen Lieferanten und Herstellern.
- Digitale Unterzeichnung und gesicherte Protokolle zur Authentifizierung aller an einer Transaktion beteiligten Parteien.
- Optimale Flexibilität durch Browser-basierte Registrierungseinrichtungen.
- Gewährleistung der Vertraulichkeit durch verschlüsselte Kommunikation und gesicherte Speicherung der Registrierungsinformationen.

Ein Tivoli PKI-System kann auf IBM AIX/6000- und Microsoft Windows NT-Serverplattformen ausgeführt werden. Es umfasst die folgenden wichtigen Funktionen:

- Ein anerkannter Zertifikatsaussteller (Certificate Authority - CA) verwaltet die Gültigkeitsdauer digitaler Zertifikate. Zur Bestätigung der Richtigkeit eines Zertifikats unterzeichnet der CA alle von ihm ausgestellten Zertifikate digital. Außerdem unterzeichnet er Zertifikatswiderrufslisten (Certificate Revocation List - CRL), um zu bestätigen, dass ein bestimmtes Zertifikat nicht mehr gültig ist. Zur weiteren Sicherung seines Unterschriftsschlüssels können Sie Verschlüsselungshardware, die auch als Hardwaresicherheitsmodul (Hardware Security Module - HSM) bezeichnet wird, wie beispielsweise den IBM 4758 PCI Cryptographic Coprocessor einsetzen.
- Eine Registrierungsstelle (Registration Authority - RA) führt die Verwaltungsaufgaben aus, die bei der Benutzerregistrierung notwendig sind. Sie stellt sicher, dass nur solche Zertifikate ausgestellt werden, die Ihre Unternehmensaktivitäten unterstützen, und dass diese Zertifikate nur an berechtigte Benutzer ausgestellt werden. Die Verwaltungsaufgaben können über automatisierte Prozesse oder auf der Basis menschlicher Entscheidungen ausgeführt werden.

  Ähnlich wie beim CA können Sie außerdem den IBM 4758 PCI Cryptographic Coprocessor einsetzen, um den Unterschriftsschlüssel der RA zu schützen.
- Eine Web-Schnittstelle für die Registrierung vereinfacht das Abrufen von Zertifikaten für Browser, Server und andere Einheiten und Zwecke, z. B. VPN-Einheiten (VPN = Virtual Private Network), Smart Cards und die sichere Übertragung von E-Mails.

- Eine Web-Verwaltungsschnittstelle, das RA Desktop, ermöglicht berechtigten Registrierungsstellen die Genehmigung oder Zurückweisung von Registrierungsanforderungen sowie die Verwaltung von Zertifikaten nach deren Ausstellung.
- Ein Prüfsubsystem ermittelt einen Nachrichtenauthentifizierungscode (MAC) für jeden Protokolleintrag. Wenn Prüfdaten nach ihrer Aufzeichnung in der Prüfdatenbank geändert oder gelöscht werden, können Sie mit Hilfe des MAC diese Manipulation feststellen.
- Regel-Exits und Unternehmensprozessobjekte (Business Process Objects - BPOs) ermöglichen Anwendungsentwicklern die Anpassung der Registrierungsprozesse.
- Integrierte Unterstützung für eine Verschlüsselungsmaschine. Zur Authentifizierung der Kommunikation werden die Tivoli PKI-Hauptkomponenten mit einem werkseitig generierten, privaten Schlüssel unterzeichnet. Sicherheitsobjekte, z. B. Schlüssel und MACs, werden verschlüsselt und in geschützten Bereichen (so genannten KeyStores oder Schlüsselspeichern) gespeichert.
- Integrierte Unterstützung für IBM Directory. Das Directory speichert Informationen zu gültigen und zurückgewiesenen Zertifikaten in einem LDAP-kompatiblen Format.
- Integrierte Unterstützung für IBM WebSphere Application Server und IBM HTTP Server. Der Web-Server arbeitet mit dem RA-Server, um Nachrichten zu verschlüsseln, Anforderungen zu authentifizieren und Zertifikate an den gewünschten Empfänger zu übertragen.
- Integrierte Unterstützung für IBM DB2 Universal Database.

2

Übersicht

Dieses Dokument beschreibt den Betrieb und die Verwaltung des Tivoli PKI-Systems. Es wird vorausgesetzt, dass Sie in den folgenden Bereichen über ausreichende Kenntnisse verfügen:

- Betriebssystem AIX oder UNIX
- Betriebssystem Windows NT
- Systemarchitektur
- Netzverwaltung
- Datenbankverwaltung
- Web-Server-Verwaltung
- Verzeichnisverwaltung

„Informationen zur Vorgehensweise" auf Seite 5, enthält Informationen zu Betrieb und Verwaltung des Tivoli PKI-Systems. Hier erfahren Sie, wie Sie das System starten und stoppen, Kennwörter ändern, den Editor für Konfigurationsdateien verwenden, das System sichern und wiederherstellen und folgende Systemkomponenten verwalten können:

- IBM WebSphere Application Server
- IBM HTTP Server
- CA-Server
- RA-Server
- Prüfsubsystem
- IBM DB2 Universal Database (UDB)
- IBM Directory
- IBM 4758 Cryptographic Coprocessor

„Erläuterungen" auf Seite 65, enthält detaillierte technische Informationen zu den Themen, die in den Beschreibungen der Prozeduren angesprochen werden.

Der Abschnitt „Referenzinformationen" auf Seite 83 enthält Referenzinformationen, beispielsweise Parameter von Konfigurationsdateien, die Syntax von Befehlszeilendienstprogrammen sowie Informationen in Tabellenform zum Prüfsubsystem.

3

Informationen zur Vorgehensweise

Dieses Kapitel erläutert die Verwaltung von Tivoli PKI und seiner Komponenten.

Tivoli PKI verwalten

Im folgenden Abschnitt werden die Tools und Prozesse beschrieben, die bei der Verwaltung von Tivoli PKI benötigt werden.

Dies ist im Einzelnen:

- Eingabe von Befehlen über die Windows NT-Befehlszeile
- Ändern von Tivoli PKI-Kennwörtern
- Starten und Stoppen der Server-Komponenten
- Ändern von Konfigurationsdateien
- Prüfen der Tivoli PKI-Konfigurationsprotokolle
- Ändern von Tivoli PKI-IP-Adressen
- Sichern und Wiederherstellen des Systems
- Überwachen der Zertifikatsaktivität
- Aufzeichnen der Anzahl von Benutzern und Zertifikaten

Befehle unter Windows NT eingeben

Wenn Sie Tivoli PKI unter Windows NT installiert haben, gibt es für eine Reihe von Tasks keine Programmsymbole, so dass diese Tasks von einer DOS-Befehlszeile aus aufgerufen werden müssen. So muss beispielsweise add_rauser manuell ausgeführt werden, damit Registratoren definiert werden können.

Wenn Sie einen Befehl angeben, für den ein Verzeichnispfad als Parameter erforderlich ist, und dieser Pfad eingebettete Leerzeichen enthält, müssen Sie den Pfad in doppelte Anführungszeichen (″) setzen. So muss beispielsweise der Parameter für den Pfad im Befehl 'add_rauser' wie folgt angegeben werden:

```
add_rauser "c:\Program Files\IBM\Trust Authority\bin"
```

Tivoli PKI-Kennwörter ändern

Tivoli PKI verfügt über ein Dienstprogramm zum Ändern von Kennwörtern. Mit diesem Dienstprogramm können Sie die während der Konfiguration des Systems definierten Standardkennwörter ändern. Ändern Sie die Kennwörter mindestens einmal nach der ersten Konfiguration des Systems und bevor Sie das System Ihren Benutzern zur Verfügung stellen.

Diese Kennwörter ermöglichen den Zugriff auf folgende Funktionskomponenten:

- Sicherer Startmechanismus

  Das Kennwort für das Steuerprogramm ermöglicht dem System, alle Tivoli PKI-Komponenten automatisch zu starten oder herunterzufahren. Außerdem kann mit diesem Kennwort auf den sicheren Start-Chiffrierschlüssel zugegriffen werden.

- Directory

  Das Directory-Administratorkennwort steuert den Zugriff auf änderbare Elemente im Directory.

- Prüf-Server

  Das Prüfadministratorkennwort ermöglicht den Zugriff auf Prüfprotokolle und Verwaltungs-Tools für Prüfoperationen.

- 4758-CA-Profil

  Das Kennwort für das 4758-CA-Profil steuert den Zugriff auf das CA-Profil des IBM SecureWay 4758 PCI Cryptographic Coprocessor.

- 4758-RA-Profil

  Das Kennwort für das 4758-RA-Profil steuert den Zugriff auf das RA-Profil des IBM SecureWay 4758 PCI Cryptographic Coprocessor.

Zum Ändern von Kennwörtern stehen Ihnen verschiedene Methoden zur Verfügung. Wenn Sie Tivoli PKI auf einer AIX-Plattform installiert haben, müssen Sie die unter „Befehlszeilenprozedur" beschriebene Befehlszeilenprozedur verwenden. Wenn Sie das Produkt auf einer Windows NT-Plattform ausführen, können Sie entweder die unter „Vorgehensweise anhand von Programmsymbolen unter Windows NT" auf Seite 7 beschriebene Prozedur oder die Befehlszeilenprozedur verwenden, um das Dienstprogramm 'Change Password' auszuführen.

Befehlszeilenprozedur

1. Wechseln Sie in das Tivoli PKI-Verzeichnis 'bin', indem Sie einen der folgenden Pfade eingeben:

   - Unter AIX lautet der Standardpfad:

     ```
     /usr/lpp/iau/bin
     ```

   - Unter Windows NT lautet der Standardpfad:

     ```
     c:\Program Files\IBM\Trust Authority\bin
     ```

2. Geben Sie je nach Betriebssystem einen der folgenden Befehle ein:

   - Unter AIX:

     changePWD.sh

   - Unter Windows NT:

     changePWD.bat

   Das folgende Menü wird angezeigt:

```
------------------------ Tivoli PKI-Kennwörter ändern ------------------------
Geben Sie die Nummer der Zusatzeinrichtung für die zu ändernde Komponente ein.
Sie werden aufgefordert, das aktuelle Kennwort und anschließend das
neue Kennwort einzugeben.
------------------------------------------------------------------------------
Kennwort ändern für
1) Beenden
```

```
2) Steuerprogramm
3) Directory-Administrator
4) Prüfadministrator
5) 4758-CA-Profil
6) 4758-RA-Profil
Option eingeben:
```

3. Wählen Sie die Option für das zu ändernde Kennwort aus, indem Sie im Feld 'Option eingeben' die entsprechende Zahl eingeben.
4. Geben Sie nach Aufforderung das aktuelle Kennwort für die ausgewählte Option ein, und bestätigen Sie es.

   Anmerkung: Bei der erstmaligen Nutzung dieses Tools müssen Sie als aktuelles Kennwort das Kennwort eingeben, das bei der Konfiguration des Systems definiert wurde. Geben Sie als Kennwort für das Steuerprogramm und den Prüfadministrator das Kennwort für das Steuerprogramm an, das Sie im Programm 'CfgPostInstall' als aktuelles Kennwort definiert haben. Als Kennwort für den Directory-Administrator, das 4758-CA-Profil und das 4758-RA-Profil geben Sie jeweils das Kennwort an, das Sie im Setup Wizard als aktuelles Kennwort definiert haben.
5. Geben Sie nach Aufforderung das neue Kennwort für die ausgewählte Option ein, und bestätigen Sie es.

   Das Kennwort darf maximal acht Zeichen lang sein (das Kennwort für das 4758-CA-Profil bzw. das 4758-RA-Profil muss genau acht Zeichen umfassen).

   Das Dienstprogramm gibt in einer Nachricht an, ob die Änderung erfolgreich war.

Nach dem erfolgreichen Abschluss der Verarbeitung ruft das Dienstprogramm das Hauptmenü erneut auf.

Anmerkung: Nachdem Sie ein Kennwort geändert haben, müssen Sie Tivoli PKI stoppen und anschließend erneut starten.

Vorgehensweise anhand von Programmsymbolen unter Windows NT

Wenn Sie Tivoli PKI auf einer Windows NT-Plattform ausführen und das Auswählen von Programmsymbolen gegenüber der Befehlseingabe in einem DOS-Befehlsfenster bevorzugen, können Sie anhand der folgenden Prozedur das Dienstprogramm 'Change Password' ausführen:

1. Wählen Sie nacheinander **Start → Programme → IBM SecureWay Trust Authority → Change Passwords Tool** aus.

   Das Menü 'Tivoli PKI-Kennwörter ändern' wird aufgerufen.
2. Führen Sie die Schritte aus, beginnend mit 3 unter „Befehlszeilenprozedur" auf Seite 6.

Serverkomponenten starten und stoppen

Tivoli PKI verwendet einen sicheren, automatischen Startmechanismus, der als Tivoli PKI-Steuerprogramm bezeichnet wird, um alle Komponenten einer Maschine zu starten oder zu stoppen. Das Tivoli PKI-Steuerprogramm (bei fernen Maschinen ein Programm pro Maschine) verfügt über einen eigenen Chiffrierschlüssel, mit dem Komponentenkennwörter bei Bedarf ver- oder entschlüsselt werden. Wenn Sie Tivoli PKI-Server-Komponenten auf fernen Maschinen installiert haben, finden Sie im Abschnitt „Ferne Server starten und stoppen” auf Seite 9 weitere Informationen.

Serverkomponenten lokal starten und stoppen

Um alle Komponenten einer Maschine zu starten oder zu stoppen, können Sie eine der folgenden Methoden verwenden:

- Geben Sie unter AIX die folgenden Befehle ein, um die Server-Komponenten zu starten oder zu stoppen. Befolgen Sie die Onlineanweisungen zur Eingabe des Kennworts für das Steuerprogramm. Bitte beachten Sie, dass Sie sich als Tivoli PKI-Konfigurationsbenutzer (cfguser) anmelden müssen, um das System zu starten und zu stoppen.

  ```
  cd /usr/lpp/iau/bin
  Start_TA.sh
  oder
  Stop_TA.sh
  ```

- Wenn Sie Tivoli PKI auf einer Windows NT-Plattform installiert haben, können Sie das entsprechende Symbol im Windows NT-Programmmenü auswählen. Sie können beispielsweise Folgendes auswählen:

  ```
  Start > Programme > IBM SecureWay Trust Authority > Trust Authority starten
  Start > Programme > IBM SecureWay Trust Authority > Trust Authority stoppen
  ```

- Wenn Sie unter Windows NT die Befehlseingabe verwenden möchten, geben Sie die folgenden Befehle in einer DOS-Befehlszeile ein, um die Serverkomponenten zu starten bzw. zu stoppen. Befolgen Sie die Online-Anweisungen zur Eingabe des Kennworts für das Steuerprogramm.

  ```
  Start_TA.bat
  oder
  Stop_TA.bat
  ```

Richtlinien zur Verwendung unter AIX

Die Richtlinien zum Starten und Stoppen des Systems unter AIX sehen folgendermaßen aus:

- Wenn der CA- und der RA-Server durch die Ausführung des Steuerprogramms unter AIX nicht gestoppt werden können, erstellen Sie mit dem Befehl **ps** eine Liste der aktiven Prozesse, und stoppen Sie diese Prozesse anschließend mit dem Befehl **kill**. Nachfolgend sind Beispiele für die Verwendung dieser Befehle sowie Beispiele für Ausgabedaten aufgeführt:

  ```
  $ ps -ef | grep irgAutoCA
  root 18886     1   0   Oct 24      - 76:34 /usr/lpp/iau/bin/irgAutoCa
     /usr/lpp/iau/etc/TrustAuthority/irgAutoCA.ini
  cfguser 23316 32400   2 11:58:20  pts/4  0:00 grep irgAutoCA
  $ kill 18886

  $ ps -ef | grep irgrasvr
  root 23526     1  12   Oct 24      - 207:46 /usr/lpp/iau/bin/irgrasvr -c
     /usr/lpp/iau/pkrf/etc/domain.cfg -d YourDomain
  cfguser 26016 12488   3 11:57:16  pts/0  0:00 grep irgrasvr
  $ kill 23526
  ```

- Durch das Stoppen von Tivoli PKI werden die Webserverprogramme unter AIX normalerweise automatisch gestoppt. Ist dies nicht der Fall, ermitteln Sie mit dem Befehl **ps** die Prozess-ID des für die jeweilige Domäne zu stoppenden Exemplars, und verwenden Sie anschließend den Befehl **kill**, um das Exemplar zu stoppen. Beispiel:

  ```
  ps -ef | grep httpServer | grep ihre_domäne
  kill prozess-id
  ```

- Durch das Stoppen von Tivoli PKI wird die Anwendungsdomäne von Tivoli PKI innerhalb von WebSphere unter AIX normalerweise automatisch gestoppt. Falls die Tivoli PKI-Anwendung nicht gestoppt wird und das Script 'Stop_TA.sh' einen Fehler während des Stoppens der Anwendungsdomäne von Tivoli PKI in WebSphere unter AIX angibt, können Sie die gesamte Anwendungsdomäne von Tivoli PKI über die Verwaltungskonsole von WebSphere stoppen. Informationen zur Verwendung der Verwaltungskonsole von WebSphere finden Sie in der WebSphere-Dokumentation.

- Durch das Starten und Stoppen von Tivoli PKI wird auch der Directory-Server automatisch gestartet bzw. ge-
  stoppt. Wenn das Directory nicht automatisch gestartet bzw. gestoppt werden soll, müssen Sie den Abschnitt [AutoStopN] der Datei 'TrustAuthControl.cfg' editieren, um den Eintrag für die Directory-Komponente zu entfernen.

Richtlinien zur Verwendung unter Windows NT

Die Richtlinien zum Starten und Stoppen des Systems unter Windows NT sehen folgendermaßen aus:

- Durch das Stoppen von Tivoli PKI werden die Web-Server-Programme unter Windows NT nicht automatisch gestoppt. Nach dem Stoppen von Tivoli PKI müssen Sie das WebSphere-Exemplar, das für die Registrierungsdomäne gestartet wurde, manuell stoppen. Verwenden Sie hierzu den Windows NT-Task-Manager, um den java.exe- und den reqdbagent.exe-Prozess zu beenden.
- Um eine optimale Leistung zu erhalten, sollten Sie vor einem erneuten Starten der Server-Komponenten auf einem Windows NT-System einen Neustart der Maschine durchführen.
- Wenn Sie das Steuerprogramm verwenden, um die Tivoli PKI-Server-Komponenten unter Windows NT zu starten, kann das Fenster, in dem das Programm gestartet wird, nicht geschlossen werden. Dies liegt daran, dass einige Komponenten diesem Konsolfenster zugeordnet sind. Nach dem Stoppen der Tivoli PKI-Serverkomponenten kann dieses Fenster geschlossen werden.
- Durch das Starten und Stoppen von Tivoli PKI wird auch der Directory-Server automatisch gestartet bzw. gestoppt. Wenn das Directory nicht automatisch gestartet bzw. gestoppt werden soll, müssen Sie den Abschnitt [AutoStopN] der Datei 'TrustAuthControl.cfg' editieren, um den Eintrag für die Directory-Komponente zu entfernen.

Ferne Server starten und stoppen

Wenn Sie die Tivoli PKI-Komponenten auf fernen Maschinen installiert haben, müssen Sie das Steuerprogramm verwenden, um die Komponenten auf den einzelnen Maschinen zu starten oder zu stoppen. Starten Sie ferne Komponenten in der folgenden Reihenfolge:

1. Directory-Server
2. CA- und Prüf-Server
3. RA-Server (einschließlich IBM HTTP Server und WebSphere Application Server)

Zum Stoppen des Systems müssen die Server-Programme in der umgekehrten Reihenfolge gestoppt werden.

Tivoli PKI-IP-Adressen ändern

Wurde das Tivoli PKI-System mit einem einzigen Host-Namen auf einer einzigen Maschine installiert und konfiguriert, können Sie die IP-Adresse dieser Maschine mit folgender Prozedur ändern:

1. Stoppen Sie das Tivoli PKI-System.
2. Ändern Sie die IP-Adresse der Maschine gemäß den Regeln Ihres Unternehmens.
3. Editieren und ändern Sie die IP-Adresse, auf die in der Datei '/usr/lpp/iau/pkrf/Domains/YourDomain/etc/httpd-RD_0.conf' verwiesen wird, und geben Sie die neue IP-Adresse an.
4. Fahren Sie die Maschine herunter, und starten Sie sie erneut.
5. Starten Sie das Tivoli PKI-System.

System sichern und wiederherstellen

Dieser Abschnitt behandelt die Sicherung und Wiederherstellung von Tivoli PKI. Folgende Themen werden ausführlich behandelt:

- Richtlinien für das Sichern und Wiederherstellen der Tivoli PKI-Datenbanken.
- Sichern und Wiederherstellen der Betriebssysteme AIX und Windows NT.
- Klonen des IBM SecureWay 4758 PCI Cryptographic Coprocessor

Sichern und Wiederherstellen unter AIX und Windows NT

Um Tivoli PKI unter AIX oder Windows NT sichern zu können, müssen Sie zunächst alle Tivoli PKI-Prozesse in der folgenden Reihenfolge beenden:

1. Tivoli PKI
2. DB2-Datenbanken

Datenbanken müssen unabhängig vom verwendeten Sicherungsdienstprogramm heruntergefahren werden. Der Directory-Server und DB2 verwenden asynchrone Schreibzugriffe. Solange diese Prozesse nicht heruntergefahren sind, kann nicht gewährleistet werden, dass die Daten in den Speicherpuffern mitgesichert werden. Je näher Sie das System an einen Einzelbenutzer-Wartungsmodus heranführen, desto besser wird die Datensicherung.

Informationen zum Stoppen und Starten von Tivoli PKI finden Sie im Abschnitt „Serverkomponenten starten und stoppen" auf Seite 8. Informationen zum Stoppen und Starten der Datenbanken finden Sie im Handbuch *IBM DB2 Universal Database Command Reference*.

Verwenden Sie die folgenden Sicherungsdienstprogramme:

- Nutzen Sie unter AIX die systeminternen Sicherungsdienstprogramme 'mksysb' und 'savevg' oder ADSM (ein weiteres IBM Produkt). Die korrekten Prozeduren für die Sicherungsdienstprogramme 'mksysb' und 'savevg' entnehmen Sie bitte Ihrer AIX-Dokumentation. Verwenden Sie ADSM nur gemeinsam mit 'mksysb'.
- Nutzen Sie unter Windows NT ein beliebiges Produkt, das in der Lage ist, ein Systemimage zu erstellen, mit dem Sie das gesamte System wiederherstellen können. Verwenden Sie ADSM nur gemeinsam mit mit dem jeweiligen Systemabbild-Dienstprogramm.

Befolgen Sie die Wiederherstellungsanweisungen des jeweiligen Dienstprogramms.

IBM 4758 PCI Cryptographic Coprocessor klonen

Zum Sichern des IBM 4758 Cryptographic Coprocessor müssen Sie den Hauptschlüssel der Maschine, auf der das Tivoli PKI-System installiert ist, auf einer anderen Maschine klonen. Beschreibungen der entsprechenden Prozeduren finden Sie in der Dokumentation zur Einheit IBM 4758, die Sie unter der folgenden Webadresse aufrufen können:

`http://www.ibm.com/security/cryptocards`

Anzahl von Benutzern und Zertifikaten überwachen

Im Rahmen der Lizenzvereinbarung müssen Sie die Anzahl der Tivoli PKI-Benutzer überwachen. Um Sie bei dieser Aufgabe zu unterstützen, stellt Tivoli PKI ein Tool zur Erstellung von Nutzungsberichten (Usage Report) zur Verfügung. Dieses Tool zeichnet die Anzahl der aktiven und inaktiven Benutzer im jeweiligen System auf sowie die Anzahl der aktiven und widerrufenen Zertifikate, die vom Tivoli PKI-CA seit der Installation des Produktes unterzeichnet worden sind. Es folgt eine Beschreibung der spezifischen Datenelemente des Nutzungsberichts (Usage Report):

Aktive Benutzer
: Benutzer mit mindestens einem aktiven Zertifikat, wobei *Benutzer* als Entität definiert ist, die über einen eindeutigen registrierten Namen (DN) verfügt.

Inaktive Benutzer
: Benutzer, die über keine aktiven Zertifikate verfügen, d. h. alle zuvor für diese Benutzer ausgestellten Zertifikate sind entweder abgelaufen oder wurden widerrufen.

Aktive Zertifikate
: Vom Tivoli PKI-CA unterzeichnete Zertifikate, die weder abgelaufen sind noch widerrufen wurden.

Widerrufene Zertifikate
: Zertifikate, die widerrufen wurden.

Vorgehensweise anhand von Programmsymbolen unter Windows NT

Wenn Sie Tivoli PKI auf einer Windows NT-Plattform ausführen und das Auswählen von Programmsymbolen gegenüber der Befehlseingabe in einem DOS-Befehlsfenster bevorzugen, können Sie anhand der folgenden Prozedur einen Nutzungsbericht (Usage Report) erstellen: Der Abschnitt „Beispielausgabe - Nutzungsbericht (Usage Report)” auf Seite 12 enthält ein Beispiel einer Berichtsausgabe.

1. Melden Sie sich als Tivoli PKI-Konfigurationsbenutzer an der Maschine an, auf der die Tivoli PKI-CA-Server-Komponente installiert ist. Der empfohlene Benutzername, der gleichzeitig auch der Standardbenutzername ist, lautet **cfguser**; möglicherweise wurde jedoch vom jeweiligen Unternehmen ein anderer Benutzername verwendet.
2. Wählen Sie **Start → Programme → IBM SecureWay Trust Authority → Trust Authority Usage Report** aus.

Befehlszeilenprozedur

Wenn Sie Tivoli PKI auf einer AIX-Plattform ausführen oder die Befehlseingabe gegenüber dem Auswählen von Programmsymbolen unter Windows NT bevorzugen, können Sie anhand der folgenden Prozedur einen Nutzungsbericht (Usage Report) erstellen: Der Abschnitt „Beispielausgabe - Nutzungsbericht (Usage Report)” auf Seite 12 enthält ein Beispiel einer Berichtsausgabe.

1. Melden Sie sich als Tivoli PKI-Konfigurationsbenutzer an der Maschine an, auf der die Tivoli PKI-CA-Server-Komponente installiert ist. Der empfohlene Benutzername, der gleichzeitig auch der Standardbenutzername ist, lautet **cfguser**. Wenn Sie Tivoli PKI unter Windows NT installiert haben, wurde vom jeweiligen Unternehmen möglicherweise ein anderer Benutzername verwendet.
2. Wechseln Sie in das Unterverzeichnis 'bin' des Tivoli PKI-Installationsverzeichnisses. In den folgenden Beispielen wird der Standardverzeichnispfad verwendet:
   - Unter AIX:
     ```
     /usr/lpp/iau/bin
     ```
   - Unter Windows NT:
     ```
     c:\Program Files\IBM\Trust Authority\bin
     ```
3. Geben Sie den folgenden Befehl ein:
   ```
   TAUsageReport
   ```

Beispielausgabe - Nutzungsbericht (Usage Report)

```
Tivoli PKI  Usage Report

Report generated on   :  Sep 28, 1999 16:10:20 EDT

    Total active users          =       42
    Total active certificates   =       53
    Total inactive users        =        6
    Total revoked certificates  =        3
```

Zertifikataktivität überwachen

Mit Hilfe des Tivoli PKI-Dienstprogramms 'Activity Report' können Sie Aktivitätsberichte erstellen, um die Anzahl der Zertifikate zu überwachen, die an einem bestimmten Tag oder innerhalb einer bestimmten Woche genehmigt, zurückgewiesen oder widerrufen wurden. Der Aktivitätsbericht (Activity Report) ist in zwei Teile untergliedert:

- Teil 1
  Im ersten Teil werden die Registratoren (RA-Administratoren) des jeweiligen Systems aufgeführt und die Zertifikatsaktivitäten der einzelnen Registratoren (Administratoren) aufgezeigt.
- Teil 2
  Im zweiten Teil des Berichts wird die Gesamtzahl der Zertifikate aufgeführt, die während des angeforderten Zeitraums genehmigt, zurückgewiesen oder widerrufen wurden. Dabei spielt es keine Rolle, ob diese Aktionen manuell durch einen Registrator oder automatisch über Regel-Exits ausgeführt wurden.

Vorgehensweise anhand von Programmsymbolen unter Windows NT

Wenn Sie Tivoli PKI auf einer Windows NT-Plattform ausführen und das Auswählen von Programmsymbolen gegenüber der Befehlseingabe in einem DOS-Befehlsfenster bevorzugen, können Sie anhand der folgenden Prozedur einen Aktivitätsbericht (Activity Report) erstellen: Der Abschnitt „Beispielausgabe - Aktivitätsbericht (Activity Report)" auf Seite 14 enthält ein Beispiel einer Berichtsausgabe.

1. Melden Sie sich als Tivoli PKI-Konfigurationsbenutzer an der Maschine an, auf der die Tivoli PKI-RA-Server-Komponente installiert ist. Der empfohlene Benutzername lautet **cfguser**; möglicherweise wurde jedoch vom jeweiligen Unternehmen ein anderer Benutzername verwendet.

2. Wählen Sie **Start → Programme → IBM SecureWay Trust Authority → Trust Authority Activity Report** aus.
3. Wenn Sie vom System aufgefordert werden, die Berichtsart einzugeben, geben Sie **1** für einen wöchentlichen Bericht ein oder **2**, um eine Zusammenfassung der Aktivitäten anzuzeigen, die an einem bestimmten Tag stattfanden.
4. Wenn Sie zur Eingabe des Datums aufgefordert werden, geben Sie das Startdatum für die Woche ein, für die ein Bericht erstellt werden soll bzw. das exakte Datum für die Erstellung eines Tagesberichts. Geben Sie das Datum im Format jjjj-mm-tt ein, beispielsweise 1999-10-01.

Befehlszeilenprozedur

Wenn Sie Tivoli PKI auf einer AIX-Plattform ausführen oder die Befehlseingabe gegenüber dem Auswählen von Programmsymbolen unter Windows NT bevorzugen, können Sie anhand der folgenden Prozedur einen Aktivitätsbericht (Activity Report) erstellen: Der Abschnitt „Beispielausgabe - Aktivitätsbericht (Activity Report)” auf Seite 14 enthält ein Beispiel einer Berichtsausgabe.

1. Melden Sie sich als Tivoli PKI-Konfigurationsbenutzer an der Maschine an, auf der die Tivoli PKI-RA-Server-Komponente installiert ist. Der empfohlene Benutzername, der gleichzeitig auch der Standardbenutzername ist, lautet **cfguser**. Wenn Sie Tivoli PKI unter Windows NT installiert haben, wurde vom jeweiligen Unternehmen möglicherweise ein anderer Benutzername verwendet.
2. Wechseln Sie in das Unterverzeichnis ’bin’ des Tivoli PKI-Installationsverzeichnisses. In den folgenden Beispielen wird der Standardverzeichnispfad verwendet:
   - Unter AIX:
     ```
     /usr/lpp/iau/bin
     ```
   - Unter Windows NT:
     ```
     c:\Program Files\IBM\Trust Authority\bin
     ```
3. Geben Sie den folgenden Befehl ein:
   ```
   TAActivityReport
   ```
4. Wenn Sie vom System aufgefordert werden, die Berichtsart einzugeben, geben Sie **1** für einen wöchentlichen Bericht ein oder **2**, um eine Zusammenfassung der Aktivitäten anzuzeigen, die an einem bestimmten Tag stattfanden.
5. Wenn Sie zur Eingabe des Datums aufgefordert werden, geben Sie das Startdatum für die Woche ein, für die ein Bericht erstellt werden soll bzw. das exakte Datum für die Erstellung eines Tagesberichts. Geben Sie das Datum im Format jjjj-mm-tt ein, beispielsweise 1999-10-01.

Anmerkung: Um die Eingabeaufforderungen zu umgehen, können Sie die folgenden Befehlsparameter in der Befehlszeile angeben:

```
TAActivityReport
[-t reportType(1/2)] [-d startDate(jjjj-mm-tt)]
```

Beispiel: **`TAActivityReport -t 2 -d 1999-09-27`**

Beispielausgabe - Aktivitätsbericht (Activity Report)

Im folgenden Beispiel wird ein täglicher Aktivitätsbericht dargestellt. Der wöchentliche Bericht ist entsprechend aufgebaut, enthält jedoch eine Zusammenfassung der wöchentlichen Summen der jeweiligen Aktivitäten.

```
Tivoli PKI Activity Report

Report generated on         : Sep 28, 1999 15:59:23 EDT
Date of daily report        : 1999-09-27

Daily Activity Report for RA Administrators

  RA Administrator DN                  Approved          Rejected          Revoked

  CN=RAadmin1, OU=PKI, O=IBM, C=US           23                 6                1
  CN=RAadmin2, OU=PKI, O=IBM, C=US           14                 2                0
  CN=RAadmin3, OU=PKI, O=IBM, C=US           55                 8                4

Daily Activity Report for the System

  Approved    =      92
  Rejected    =      16
  Revoked     =       5
```

WebSphere Application Server verwalten

IBM WebSphere besteht aus einer Gruppe von Softwareprodukten, mit denen Unternehmen leistungsfähige Web-Sites entwickeln und verwalten können. Der WebSphere Application Server stellt zusammen mit dem IBM HTTP Server in Tivoli PKI die Infrastruktur für Web-Server-Funktionalität bereit.

Status des WebSphere Application Server prüfen

Je nach Umgebung können Sie den Status des WebSphere Application Server mit folgenden Prozeduren prüfen:

- Unter AIX:
  1. Melden Sie sich bei AIX als Root an.
  2. Prüfen Sie die Prozesstabelle, und suchen Sie nach der folgenden Zeichenfolge:

     ```
     ManagedServer
     ```

     Wenn Sie diesen Prozess finden, fahren Sie mit Schritt 3 fort. Finden Sie diesen Prozess nicht, lesen Sie bitte im Abschnitt „Fehlerbehebung” auf Seite 135 nach.
  3. Informationen dazu, wie Sie die Verwaltungskonsole von WebSphere verwenden und den Serverstatus bestimmen können, finden Sie in der WebSphere-Dokumentation.
- Unter Windows NT:
  1. Melden Sie sich bei Windows NT als Systemadministrator an.
  2. Starten Sie den Task-Manager durch Drücken der Tastenkombination **Strg Alt** und **Entf**.
  3. Wählen Sie die Registerkarte **Prozesse** aus.
  4. Suchen Sie nach mindestens einem Vorkommen des Prozesses java.exe.

     Finden Sie diesen Prozess, fahren Sie mit Schritt 5 auf Seite 15 fort. Finden Sie diesen Prozess nicht, lesen Sie bitte im Abschnitt „Fehlerbehebung” auf Seite 135 nach.

5. Informationen zum Zugriff auf die WebSphere-Verwaltungsseiten und zur Ermittlung des Server-Status finden Sie in der WebSphere-Dokumentation.

WebSphere Application Server-Protokolle prüfen

Sie können die Protokolle prüfen, in denen die Transaktionen zwischen dem WebSphere Application Server und dem Tivoli PKI Setup Wizard aufgezeichnet werden. Die Positionen dieser Protokolle sind in Tabelle 1 dargestellt.

Tabelle 1. WebSphere Application Server-Protokolle über Transaktionen mit dem Setup Wizard

AIX-Standardpfad	Windows NT-Standardpfad	Anmerkungen
/usr/WebSphere/AppServer/logs/TivoliPKI-Cfg_stderr.log	c:\Program Files\IBM\Trust Authority\etc\logs\jvm_stderr.log	Standardausgabepfad für Fehlernachrichten der Java Virtual Machine (JVM)
/usr/WebSphere/AppServer/logs/TivoliPKI-Cfg_stdout.log	c:\Program Files\IBM\Trust Authority\etc\logs\jvm_stdout.log	Standardausgabepfad der JVM

Sie können die Protokolle prüfen, die die Transaktionen zwischen dem IBM WebSphere Application Server und Ihrer Registrierungsanwendung aufzeichnen. Die Positionen dieser Protokolle werden in Tabelle 2 erläutert.

Tabelle 2. IBM WebSphere Application Server - Protokolle über Transaktionen mit der Registrierungsanwendung

AIX-Standardpfad	Windows NT-Standardpfad	Anmerkungen
/usr/WebSphere/AppServer/logs/TivoliPKI_stderr.log	c:\Program Files\IBM\Trust Authority\pkrf\Domains\YourDomain\etc\logs\jvm_stderr.log	Standardausgabepfad für Fehlernachrichten der Java Virtual Machine (JVM)
/usr/WebSphere/AppServer/logs/TivoliPKI_stdout.log	c:\Program Files\IBM\Trust Authority\pkrf\Domains\YourDomain\n\etc\logs\jvm_stdout.log	Standardausgabepfad der JVM

HTTP Server verwalten

IBM HTTP Server ist das Web-Server-Produkt, das die web-gestützte Kommunikation mit Browsern und anderen Programmen verwaltet. Der HTTP-Dämon (HTTPD) ist die Hauptkomponente des Web-Servers. Tivoli PKI verwendet mehrere HTTP-Dämonen. Diese HTTP-Dämonexemplare verwalten öffentliche, verschlüsselte sowie vom Client authentifizierte und verschlüsselte Verbindungen. Detaillierte Informationen zu Web-Servern und zu den verschiedenen Verbindungsarten, die in Tivoli PKI zur Verwaltung unterschiedlicher Transaktionen eingesetzt werden, finden Sie im Abschnitt „Webserver” auf Seite 79.

Status des HTTP Server prüfen

Je nach Umgebung können Sie den Status des HTTP Server mit folgenden Prozeduren prüfen:

- Unter AIX:
  1. Melden Sie sich bei AIX als Root an.
  2. Prüfen Sie die Prozesstabelle und suchen Sie nach folgender Zeichenfolge:
     - `sidd` (einmal)
     - `httpd` (mindestens zweimal)

     Sind diese drei Prozesse vorhanden, fahren Sie mit Schritt 3 fort. Sind nicht alle dieser drei Prozesse vorhanden, lesen Sie bitte im Abschnitt „Fehlerbehebung” auf Seite 135 nach.
  3. Wechseln Sie in das Verzeichnis 'bin'. Dieses Verzeichnis hat folgenden Standardpfad:
     ```
     /usr/lpp/iau/bin
     ```
  4. Prüfen Sie die Ports, indem Sie für jeden Port folgenden Befehl eingeben:
     ```
     checkSrvPortStatus -p Port -s Server -r1 -w1 -i
     ```

     Hierbei steht *Port* für die Nummer des zu prüfenden Ports und *Server* für den Namen des zugeordneten HTTP Servers. Eine Übersicht der standardmäßigen HTTP Server- und Port-Konfigurationen von Tivoli PKI finden Sie in Tabelle 11 auf Seite 80.

     Ist die Antwort des geprüften Ports erfolgreich, wird folgende Nachricht angezeigt:
     ```
     Port:Port on  Server is bound.
     ```

     Hierbei steht *Port* für den geprüften Port und *Server* für den Namen des entsprechenden Servers.
- Unter Windows NT:
  1. Melden Sie sich bei Windows NT als Systemadministrator an.
  2. Starten Sie den Task-Manager durch Drücken der Tastenkombination **Strg**, **Alt** und **Entf**.
  3. Wählen Sie die Registerkarte **Prozesse** aus.
  4. Suchen Sie nach zwei Exemplaren des Prozesses Apache.exe.

     Sind diese zwei Prozesse vorhanden, fahren Sie mit Schritt 5 fort. Sind diese beiden Prozesse nicht vorhanden, lesen Sie bitte im Abschnitt „Fehlerbehebung” auf Seite 135 nach.
  5. Wechseln Sie an der MS DOS-Eingabeaufforderung in das Verzeichnis 'bin'. Dieses Verzeichnis hat folgenden Standardpfad:
     ```
     c:\Program Files\IBM\Trust Authority\bin
     ```

6. Prüfen Sie die Ports, indem Sie für jeden Port folgenden Befehl eingeben:

   ```
   checkSrvPortStatus -p Port -s
    Server -r1 -w1 -i
   ```

   Hierbei steht *Port* für die Nummer des zu prüfenden Ports und *Server* für den Namen des zugeordneten HTTP Servers. Eine Übersicht der standardmäßigen HTTP Server- und Port-Konfigurationen von Tivoli PKI finden Sie in Tabelle 11 auf Seite 80.

   Ist die Antwort des geprüften Ports erfolgreich, wird folgende Nachricht angezeigt:

   ```
   Port:Port on  Server is bound.
   ```

   Hierbei steht *Port* für den geprüften Port und *Server* für den Namen des entsprechenden Servers.

HTTP Server-Protokolle prüfen

Sie können die Protokolle prüfen, die Transaktionen zwischen dem IBM HTTP Server und dem Tivoli PKI Setup Wizard aufzeichnen. Namen und Positionen der entsprechenden Protokolle finden Sie in der WebSphere-Dokumentation.

Außerdem können Sie das Protokoll prüfen, das Transaktionen zwischen dem IBM HTTP Server und Ihrer Registrierungsanwendung aufzeichnet. Die Position dieses Protokolls ist in Tabelle 3 angegeben.

Tabelle 3. HTTP Server-Protokoll

AIX-Standardpfad	Windows NT-Standardpfad	Anmerkungen
/usr/HTTPServer/logs/error_log	c:\Program Files\IBM\Trust Authority\Domains\YourDomain\ logs\apache.log.ERROR.PID	Fehlernachrichten des IBM HTTP Server

CA-Server verwalten

In diesem Abschnitt werden Prozeduren für Betrieb und Verwaltung des Tivoli PKI Zertifikatsaussteller-Servers (CA-Server) erläutert. Der CA-Server verwaltet die server-seitigen Tasks für den Tivoli PKI-CA. Er befindet sich zusammen mit seinem DB2-Datenbankexemplar auf einer lokalen oder fernen Maschine.

Die folgenden Tasks zur Verwaltung des CA-Servers werden beschrieben:

- Änderung der folgenden Angaben in der Konfigurationsdatei 'jonahca.ini' mit einem Texteditor:
  - Änderung des TCP-Listener-Ports für den CA
  - Änderung des Sendeaufrufintervalls für PKIX-Nachrichten
  - Änderung der CRL-Einstellungen
  - Änderung der ICL-Schutzregel
- Änderung des ICL-Schutzschlüssels
- Prüfung der Integrität der CA-Serverdatenbank
- Verwendung des Dienstprogramms 'CA Certification' für gegenseitige Zertifizierungen und CA-Hierarchien.

- Prüfung der CA-Serverprotokolle.
- Prüfung des Status des CA-Servers
- Aktivierung der CRL-Verteilungspunkte

Listener-Port des CA-Servers ändern

Der Listener-Port des CA-Servers ist der Port, an dem der CA für PKIX-Nachrichten empfangsbereit ist. So können Sie den Wert für diesen Port ändern:

1. Melden Sie sich bei Ihrem Betriebssystem als Systemadministrator an.
2. Stoppen Sie das Tivoli PKI-System. Lesen Sie gegebenenfalls die Anweisungen unter „Serverkomponenten starten und stoppen” auf Seite 8 nach.
3. Laden Sie die Konfigurationsdatei ’jonahca.ini’ in einen Texteditor. Informationen zu den Dateipositionen unter AIX und Windows NT finden Sie in Tabelle 12 auf Seite 84.
4. Editieren Sie im Abschnitt **Transport** den Parameter **TCPPort**.
5. Ändern Sie den Wert der Port-Nummer.
6. Speichern Sie die Datei.
7. Laden Sie die Konfigurationsdatei ’jonahra.ini’ in einen Texteditor. (Diese Datei kann sich je nach vorhandener Installation auf einer lokalen oder einer fernen Maschine befinden.).
8. Ändern Sie im Abschnitt **URLs** den Wert der Port-Nummer.
9. Editieren Sie im Abschnitt **General** den Parameter **Issuer1URL1**.
10. Ändern Sie den Wert der Port-Nummer.
11. Speichern Sie die Datei.
12. Starten Sie das Tivoli PKI-System.

CA-Sendeaufrufintervall ändern

Das CA-Sendeaufrufintervall ist die Zeit in Sekunden (s), Minuten (m) oder Stunden (h) zwischen den Abfragen der Arbeitsablaufwarteschlange durch den CA-Server. Die Elemente in dieser Warteschlange, deren Zuteilungszeit abgelaufen ist, werden für die Verarbeitung zugeteilt. So ändern Sie das Sendeaufrufintervall:

1. Melden Sie sich bei Ihrem Betriebssystem als Systemadministrator an.
2. Stoppen Sie das Tivoli PKI-System. Lesen Sie gegebenenfalls die Anweisungen unter „Serverkomponenten starten und stoppen” auf Seite 8 nach.
3. Laden Sie die Konfigurationsdatei ’jonahca.ini’ in einen Texteditor. Informationen zu den Dateipositionen unter AIX und Windows NT finden Sie in Tabelle 12 auf Seite 84.
4. Editieren Sie im Abschnitt **Transport** den Parameter **PollInterval**.
5. Ändern Sie den Wert des Sendeaufrufintervalls.
6. Speichern Sie die Datei.
7. Starten Sie das Tivoli PKI-System.

CRL-Einstellungen ändern

Eine Zertifikatswiderrufsliste (CRL) ist eine digital unterzeichnete, mit Zeitmarken versehene Liste der Zertifikate, die vom Zertifikatsaussteller (CA) widerrufen wurden. In der Konfigurationsdatei des CA-Servers können folgende Werte geändert werden, um die Art der CRL-Verwaltung zu beeinflussen:

- Die Zeit zwischen den geplanten CRL-Erstellungen
- Die Gültigkeitsdauer einer CRL

Zulässige Zeit zwischen CRL-Erstellungen ändern

So können Sie die Regeln für Zertifikate und die gegenseitige Zertifizierung bezüglich der zulässigen Intervalle zwischen geplanten Publizierungen einer CRL ändern:

1. Melden Sie sich bei Ihrem Betriebssystem als Systemadministrator an.
2. Stoppen Sie das Tivoli PKI-System. Lesen Sie gegebenenfalls die Anweisungen unter „Serverkomponenten starten und stoppen" auf Seite 8 nach.
3. Laden Sie die Konfigurationsdatei 'jonahca.ini' in einen Texteditor. Informationen zu den Dateipositionen unter AIX und Windows NT finden Sie in Tabelle 12 auf Seite 84.
4. Editieren Sie im Abschnitt **CertPolicy** den Parameter **TimeBetweenCRLs**.
5. Ändern Sie den Wert für die Zeit zwischen den Erstellungen von neuen CRLs.

   Der Wert ist ein in Minuten (m), Stunden (h) oder Tagen (d) angegebenes Intervall. Beispiel: **1d**. Der Wert muss kleiner sein als der Wert für die Gültigkeitsdauer der CRL.
6. Editieren Sie im Abschnitt **CrossCertPolicy** den Parameter **TimeBetweenCRLs**.
7. Ändern Sie den Wert für die Zeit zwischen den Erstellungen von neuen CRLs.

   Der Wert ist ein in Minuten (m), Stunden (h) oder Tagen (d) angegebenes Intervall. Beispiel: **1d**. Der Wert muss kleiner sein als der Wert für die Gültigkeitsdauer der CRL.
8. Speichern Sie die Datei.
9. Starten Sie das Tivoli PKI-System.

Gültigkeitsdauer einer CRL ändern

So können Sie die Regeln für Zertifikate und die gegenseitige Zertifizierung bezüglich der Gültigkeitsdauer einer CRL ändern:

1. Melden Sie sich bei Ihrem Betriebssystem als Systemadministrator an.
2. Stoppen Sie das Tivoli PKI-System. Lesen Sie gegebenenfalls die Anweisungen unter „Serverkomponenten starten und stoppen" auf Seite 8 nach.
3. Laden Sie die Konfigurationsdatei 'jonahca.ini' in einen Texteditor. Informationen zu den Dateipositionen unter AIX und Windows NT finden Sie in Tabelle 12 auf Seite 84.
4. Editieren Sie im Abschnitt **CertPolicy** den Parameter **CRLDuration**.
5. Ändern Sie den Wert für die Gültigkeitsdauer einer CRL. Der Wert ist ein in Minuten (m), Stunden (h) oder Tagen (d) angegebenes Intervall. Beispiel: **2d.**
6. Editieren Sie im Abschnitt **CrossCertPolicy** den Parameter **CRLDuration**.
7. Ändern Sie den Wert für die Gültigkeitsdauer einer CRL. Der Wert ist ein in Stunden, Minuten oder Tagen angegebenes Intervall. Beispiel: **2d**.
8. Speichern Sie die Datei.
9. Starten Sie das Tivoli PKI-System.

ICL-Schutzregel ändern

Die Liste der ausgestellten Zertifikate (Issued Certificates List - ICL) enthält die ausgestellten Zertifikate zusammen mit ihrem jeweiligen Status. Beim ICL-Schutzschlüssel handelt es sich um einen chiffrierten Schlüssel, der im Tivoli PKI-Schlüsselspeicher (KeyStore) gespeichert ist und verwendet wird, um für alle Spalten der ICL MAC-Werte (Message Authentication Code - Nachrichtenauthentifizierungscode) zu berechnen. Wenn der berechnete MAC-Wert nicht mit dem gespeicherten MAC-Wert übereinstimmt, verwendet das System die ICL-Schutzregel und führt entsprechende Aktionen aus.

So ändern Sie die ICL-Schutzregel:

1. Melden Sie sich bei Ihrem Betriebssystem als Systemadministrator an.
2. Stoppen Sie das Tivoli PKI-System. Lesen Sie gegebenenfalls die Anweisungen unter „Serverkomponenten starten und stoppen" auf Seite 8 nach.
3. Laden Sie die Konfigurationsdatei 'jonahca.ini' in einen Texteditor. Informationen zu den Dateipositionen unter AIX und Windows NT finden Sie in Tabelle 12 auf Seite 84.
4. Editieren Sie im Abschnitt **ICL** den Parameter **IclProtectionPolicy**.
5. Ändern Sie den Wert der ICL-Schutzregel in einen Wert, der die Anforderungen Ihres Unternehmens erfüllt. Folgende Werte sind möglich:
   - **Ignore** — Das System ignoriert die Abweichung und zeigt keine Nachrichten an.

     Anmerkung: Dieser Wert wirkt sich auf den Betrieb des Tools CAIntegrityCheck aus (siehe „Integrität der CA-Serverdatenbank prüfen" auf Seite 21). Wenn Sie **Ignore** angeben, kann das Tool CAIntegrityCheck keinen Missbrauch ermitteln, selbst wenn ein solcher vorliegt.
   - **ContinueWithMessage** — Das System zeigt eine Warnung an, setzt die Transaktion jedoch fort.
   - **TerminateTransaction** — Das System zeigt eine Fehlernachricht an und beendet die Transaktion.
6. Speichern Sie die Datei.
7. Starten Sie das Tivoli PKI-System.

ICL-Schutzschlüssel ändern

Der ICL-Schutzschlüssel wird niemals Benutzern oder Administratoren preisgegeben. Um jedoch einem Missbrauch oder einer unbeabsichtigten Dateninkonsistenz vorzubeugen, empfiehlt es sich, den ICL-Schutzschlüssel in regelmäßigen Abständen zu ändern. Tivoli PKI stellt das Befehlszeilen-Tool **CARemac** zur Verfügung, mit dem ein neuer ICL-Schutzschlüssel zur Berechnung eines neuen MAC-Wertes generiert wird. So ändern Sie den ICL-Schutzschlüssel:

1. Wechseln Sie zu der Maschine, auf der der CA-Server installiert ist.
2. Vergewissern Sie sich, dass auf dem Tivoli PKI-System keine Aktivität besteht. Die Inaktivität können Sie mit Hilfe der Tivoli PKI-Komponentenprotokolle feststellen.

3. Führen Sie das Tool für den ICL-Schutzschlüssel unter dem Benutzerkonto 'cfguser' aus, indem Sie den Befehl **CARemac** (der den Installationspfad von Tivoli PKI enthält) in der Tivoli PKI-Befehlszeile eingeben. Beispiel:

   - Unter AIX, wenn Sie den Standardinstallationspfad von Tivoli PKI verwenden:

     ```
     CARemac in /usr/lpp/iau/bin
     ```

   - Unter Windows NT, wenn Sie den Standardinstallationspfad von Tivoli PKI verwenden:

     ```
     CARemac in "c:Program Files\IBM\Trust Authority\bin"
     ```

   Das Tool fordert Sie zur Eingabe des Kennworts für das Tivoli PKI-Steuerprogramm auf.

4. Geben Sie das Kennwort für das Tivoli PKI-Steuerprogramm ein.

Integrität der CA-Serverdatenbank prüfen

Tivoli PKI stellt das Tool CAIntegrityCheck zur Verfügung, mit dessen Hilfe Missbräuche der CA-Server-Datenbank ermittelt werden können. Unter normalen Umständen führt der CA Schutzprüfungen nur für den Teilsatz der ICL-Einträge aus, auf den zu einem bestimmten Zeitpunkt gerade zugegriffen wird. Mit anderen Worten: Der CA prüft lediglich diejenigen Einträge, die bei Erstellung der CRL ausgewählt sind, demnach also den Status *revoked* (widerrufen) haben. Daher werden die meisten der ICL-Einträge während des normalen Tivoli PKI-CA-Betriebs nicht auf ihre Integrität hin geprüft.

Wenn Sie die Integrität der gesamten CA-Datenbank prüfen wollen, müssen Sie das Tool CAIntegrityCheck verwenden. Dieses ausführbare Programm liest alle Einträge in der ICL und führt für sie entsprechende Integritätsprüfungen durch.

So können Sie die Integrität der CA-Server-Datenbank prüfen:

1. Wechseln Sie zu der Maschine, auf der der CA-Server installiert ist, und melden Sie sich als 'cfguser' an.
2. Führen Sie das Tool zur Prüfung der Integrität der CA-Datenbank (CAIntegrityCheck) aus, indem Sie in der Tivoli PKI-Befehlszeile folgenden Befehl eingeben (der den entsprechenden Tivoli PKI-Installationspfad enthält). Beispiel:

   - Unter AIX, wenn Sie den Standardinstallationspfad von Tivoli PKI verwenden:

     ```
     CAIntegrityCheck in /usr/lpp/iau/bin
     ```

   - Unter Windows NT, wenn Sie den Standardinstallationspfad von Tivoli PKI verwenden:

     ```
     CAIntegrityCheck in "c:Program Files\IBM\Trust Authority\bin"
     ```

   Das Tool fordert Sie zur Eingabe des Kennworts für das Tivoli PKI-Steuerprogramm auf.

3. Geben Sie das Kennwort für das Tivoli PKI-Steuerprogramm ein.
4. Falls das Programm CAIntegrityCheck Fehlernachrichten für den Integritätsschutz zurückgibt, führen Sie den Befehl **CARemac** erneut aus, um einen neuen Schutzschlüssel festzulegen und die Integrität der CA-Datenbank wiederherzustellen. Bitte denken Sie daran, dass bei Ausführung des Befehls **CARemac** der CA aktiv sein muss, auf dem Tivoli PKI-System jedoch keine Aktivität bestehen darf.

CA-Zertifikat über gegenseitige Zertifizierung anfordern

Sie können im Namen des Tivoli PKI-CA ein CA-Zertifikat von einem anderen CA anfordern, wenn Sie das Sicherungsmodell für die gegenseitige Zertifizierung verwenden. Die gegenseitige Zertifizierung ermöglicht es zuverlässigen CAs, die Anerkennung gegenseitig ausgestellter Zertifikate als Identitätsnachweis zu vereinbaren. Obwohl die gegenseitige Zertifizierung zwischen CAs in beiden Richtungen erfolgen kann, werden in Tivoli PKI Anforderungen für die gegenseitige Zertifizierung nur in einer Richtung unterstützt.

Anmerkung: Tivoli PKI unterstützt eine gegenseitige Zertifizierung nur zwischen CAs, die das PKIX-Zertifikatsverwaltungsprotokoll (Certificate Management Protocol, CMP) einhalten.

Verwenden Sie für die gegenseitige Zertifizierung mit einem anderen CA das Tivoli PKI-Dienstprogramm 'CA Certification' (CACertRq). Dieses Dienstprogramm ist ein Befehlszeilen-Tool. Beim Starten können Sie Optionen für die Standardzertifikatserweiterung für Namenseinschränkungen definieren. Ein kleingeschriebener Buchstabe steht für die Aufnahme in die Liste zulässiger Unterverzeichnisstrukturen. Ein großgeschriebener Buchstabe steht für die Aufnahme in die Liste nicht zulässiger Unterverzeichnisstrukturen. In der Regel werden nicht zulässige Unterverzeichnisstrukturen nur für einen Adresstyp angegeben, für den auch eine Liste zulässiger Unterverzeichnisstrukturen existiert.

Die folgenden Abschnitte beschreiben, wie Sie ein CA-Zertifikat mit Hilfe des Modells für die gegenseitige Zertifizierung anfordern können.

Schritte zur gegenseitigen Zertifizierung

Befolgen Sie die nachfolgend beschriebenen Anweisungen, um ein CA-Zertifikat mit Hilfe der gegenseitigen Zertifizierung anzufordern.

1. Führen Sie im Namen des anfordernden CA folgende Schritte gemäß den Anweisungen zur web-gestützten Registrierung im *Tivoli PKI Benutzerhandbuch* aus:
   a. Führen Sie eine Vorabregistrierung aus und geben Sie an, dass die Anforderung für einen CA erfolgt.

      Achten Sie beim Ausfüllen des Registrierungsformulars darauf, einen registrierten Namen (DN) einzugeben, der mit dem des anfordernden CA übereinstimmt.

   b. Prüfen Sie den Status der Registrierungsanforderung.

   c. Befolgen Sie die Anweisung am Ende des Abschnitts, um die Vorabregistrierungsdatei zu speichern.
2. Übertragen Sie die Vorabregistrierungsdatei auf die Maschine, auf der sich der anfordernde CA befindet.
3. Melden Sie sich bei Tivoli PKI unter dem Benutzerkonto 'cfguser' auf der Maschine an, auf der sich der CA befindet, der die gegenseitige Zertifizierung anfordert.
4. Führen Sie den Befehl **CACertRq** aus, und zwar unter AIX über die Befehlszeile und unter Windows NT über die DOS-Eingabeaufforderung.

   Stellen Sie bei Ausführung des Befehls **CACertRq** sicher, dass Sie den absoluten Pfad und den Namen der Vorabregistrierungsdatei eingeben. Informationen zur Befehlssyntax und Parameterbeschreibungen finden Sie im Abschnitt „Dienstprogramm CA Certification" auf Seite 112.

Anmerkung: Wenn Sie als Parameter eines Befehls einen Verzeichnispfad angeben, der eingebettete Leerzeichen enthält, müssen Sie den Pfad in doppelte Anführungszeichen (″ ″) setzen. Für den Befehl **CACertRq** beispielsweise würden Sie den Parameter '-r' *vorabregistrierungspfad* (mit eingebetteten Leerzeichen) folgendermaßen angeben:

```
CACertRq -d .companyA.com -r "c:\Program Files\IBM\Trust Authority\
   ccprereg.reg"  -P 1835 -W Secure99
```

IP-Adressmaske angeben

Sie können ein gegenseitig zertifiziertes CA-Zertifikat anfordern, das die Gültigkeit des Zertifikats auf die IP-Adressen einschränkt, die von Ihrem Unternehmen verwendet werden.

Im folgenden Beispiel ist das Betriebssystem AIX, Ihr Unternehmen verwendet IP-Adressen im Bereich von 9.0.0.0. bis 9.255.255.254, die Vorabregistrierungsdatei befindet sich im Pfad '/tmp/ccprereg.reg', und das Kennwort lautet 'Secure99'. Folgender Befehl platziert den angegebenen Adressenbereich in der Liste zulässiger Unterverzeichnisstrukturen:

```
CACertRq -i 9.0.0.0/255.0.0.0 -r /tmp/ccprereg.reg -P 1835 -W Secure99
```

DNS-Adressen angeben

Sie können ein gegenseitig zertifiziertes CA-Zertifikat anfordern, das die Gültigkeit des Zertifikats auf eine Gruppe von DNS-Adressen einschränkt.

Im folgenden Beispiel wird das Betriebssystem Windows NT verwendet, und alle Tivoli PKI-CA-Hosts verfügen über DNS-Adressen mit der Endung '.companyA.com'. Mit folgendem Befehl werden die angegebenen DNS-Adressen in der Liste der zulässigen Unterverzeichnisstrukturen platziert:

```
CACertRq -d .companyA.com -r c:\temp\ccprereg.reg -P 1835 -W Secure99
```

Anmerkung: Beginnt eine DNS-Adresse mit einem Punkt, werden alle Hosts einbezogen, die mit dieser Unterzeichenfolge (einschließlich des Punktes) enden. Diese Adressen werden in die Liste der Unterverzeichnisstrukturen aufgenommen. Beginnt die Adresse nicht mit einem Punkt, wird nur der Host einbezogen, dessen Name der Zeichenfolge entspricht.

Der Einschränkung '.companyA.com' entsprechen beispielsweise us.companyA.com, vnet.companyA.com und w3.software.companyA.com, jedoch nicht companyA.com (oder kidcompanyA.com) selbst. Der Einschränkung companyA.com entsprechen companyA.com, jedoch nicht us.companyA.com oder die übrigen Adressen. Daraus folgt, dass eine zulässige Unterverzeichnisstrukturen ohne führenden Punkt (.) nur einen möglichen Knoten angibt. Angaben ohne einen führenden Punkt werden primär für nicht zulässige Unterverzeichnisstrukturen verwendet.

E-Mail-Adressen angeben

Sie können ein gegenseitig zertifiziertes CA-Zertifikat anfordern, das die Gültigkeit des Zertifikats auf eine Gruppe von E-Mail-Adressen einschränkt.

Im folgenden Beispiel wird das Betriebssystem Windows NT verwendet, alle Tivoli PKI-CA-Hosts verfügen über E-Mail-Adressen, die mit .us.companyA.com enden, Pfad und Dateiname der Vorabregistrierungsdatei lauten 'a:\ccprereg.reg', und das Kennwort lautet 'Secure99'. Folgender Befehl platziert die angegebenen E-Mail-Adressen in der Liste zulässiger Unterverzeichnisstrukturen:

```
CACertRq -m .us.companyA.com -r a:\ccprereg.reg -P 1835 -W Secure99
```

Sie können ein gegenseitig zertifiziertes CA-Zertifikat anfordern, das die Gültigkeit des Zertifikats auf alle bis auf ein Element einer Gruppe von E-Mail-Adressen einschränkt.

Im folgenden Beispiel wird das Betriebssystem Windows NT verwendet, der Tivoli PKI-CA-Host hat die E-Mail-Adresse outCA.us.companyA.com, Pfad und Dateiname der Vorabregistrierungsdatei lauten 'a:\ccprereg.reg', und das Kennwort lautet 'Secure99'. Folgender Befehl platziert die angegebenen E-Mail-Adressen in der Liste nicht zulässiger Unterverzeichnisstrukturen:

```
CACertRq -m .us.companyA.com -M outCA.us.companyA.com -r a:\ccprereg.reg -P 1835
   -W Secure99
```

URIs angeben

Sie können ein gegenseitig zertifiziertes CA-Zertifikat anfordern, das die Gültigkeit des Zertifikats auf eine Gruppe von URIs (Uniform Resource Identifiers, eine Kennungskategorie, die hauptsächlich aus URL-Adressen besteht) einschränkt.

Im folgenden Beispiel wird das Betriebssystem AIX verwendet, alle Tivoli PKI-CA-Hosts verfügen über Namen, die mit .xyz.com enden, Pfad und Dateiname der Vorabregistrierungsdatei lauten '/tmp/ccprereg.reg', und das Kennwort lautet 'Secure99'. Folgender Befehl platziert die angegebene URI in der Liste zulässiger Unterverzeichnisstrukturen:

```
CACertRq -u .xyz.com -r /tmp/ccprereg.reg -P 1835 -W Secure99
```

Anmerkung: Der Knotenabschnitt (in einer Baumstruktur ein Punkt, an dem untergeordnete Datenelemente ihren Ursprung haben) der URI unterliegt den im Abschnitt „DNS-Adressen angeben" auf Seite 23 beschriebenen Regeln, sofern er keine IP-Adressen enthält. In diesem Fall wird er als exakte Übereinstimmung behandelt.

Verzeichniseinträge angeben

Sie können ein gegenseitig zertifiziertes CA-Zertifikat anfordern, das die Gültigkeit des Zertifikats auf eine Gruppe von Verzeichniseinträgen mit den gleichen RDNs (Relative Distinguished Names) einschränkt.

Im folgenden Beispiel wird das Betriebssystem AIX verwendet, alle Tivoli PKI-CA-Hosts verfügen über RDNs, die den angegebenen RDNs (/C=US/O=companyA/OU=departmentB) entsprechen, Pfad und Dateiname der Vorabregistrierungsdatei lauten '/tmp/ccprereg.reg', und das Kennwort lautet 'Secure99'. Folgender Befehl platziert den angegebenen RDN in der Liste der zulässigen Unterverzeichnisstrukturen:

```
CACertRq -n "/C=US/O=companyA/OU=departmentB" -r /tmp/ccprereg.reg -P 1835
   -W Secure99
```

CA-Zertifikat mit Hilfe des Hierarchiemodells anfordern

Sie können ein CA-Zertifikat mit Hilfe des Hierarchiemodells von einem anderen CA anfordern. Unternehmen fordern häufig CA-Zertifikate von etablierten und extrem gesicherten CAs an, um die Zuverlässigkeit ihrer eigenen CAs zu vergrößern. CAs betrachten die CAs als zuverlässig, die in der Hierarchie über ihnen stehen, und akzeptieren deren Zertifikate als Identitätsnachweis. Sie können ein CA-Zertifikat entweder von einem Fremd-CA oder von einem Tivoli PKI-CA anfordern.

Anmerkung: Tivoli PKI unterstützt eine hierarchische Zertifizierung nur zwischen CAs, die das PKIX-Zertifikatsverwaltungsprotokoll (Certificate Management Protocol, CMP) sowie die Protokolle PKCS#7 und PKCS#10 einhalten.

Zur Definition einer CA-Hierarchie verwenden Sie das Tivoli PKI-Dienstprogramm CA Certification (**CACertRq**). **Wenn Sie dieses Tool starten, müssen Sie mindestens eine Option für die Standardzertifikatserweiterung für Namenseinschränkungen definieren.** (Detaillierte Beschreibungen der Zertifikatserweiterungen finden Sie im Abschnitt „Zertifikatserweiterungen” auf Seite 67.) Ein kleingeschriebener Buchstabe steht für die Aufnahme in die Liste zulässiger Unterverzeichnisstrukturen. Ein großgeschriebener Buchstabe steht für die Aufnahme in die Liste nicht zulässiger Unterverzeichnisstrukturen. In der Regel werden nicht zulässige Unterverzeichnisstrukturen nur für einen Adresstyp angegeben, für den auch eine Liste zulässiger Unterverzeichnisstrukturen existiert.

Anmerkung: Wenn Sie planen, als Teil Ihrer allgemeinen Hierarchielösung die hierarchischen CA-Zertifikate in Netscape Communicator herunterzuladen, sollten Sie den Parameter ’-m ..’ mit dem Dienstprogramm CA Certification verwenden, um die Erweiterung für Namenseinschränkungen (Name Constraints) aus dem resultierenden CA-Zertifikat auszuschließen. Mit Ausnahme von ’-m ..’ sollten Sie keine anderen der Befehlszeilenoptionen für Namenseinschränkungen (also nicht -i/I, -d/D, -u/U, -n/N oder -m/-M) mit dem Dienstprogramm CA Certification verwenden. Die Syntax für einen solchen Befehl sieht folgendermaßen aus:

```
CACertRq -m .. -h -r
vorabregistrierungspfad -P 1835 -W
kennwort
```

Wenn Sie den Befehl für das Dienstprogramm CA Certification ausführen, wird die auf diese Weise aufgebaute Hierarchie in den folgenden Dateien gespeichert:

- CAChain.P7b
- RAsCopyOfCAChain.P7b
- CAChain.b64
- RAsCopyOfCAChain.b64

Die folgenden Abschnitte beschreiben, wie Sie ein CA-Zertifikat mit Hilfe des Hierarchiemodells anfordern können.

Schritte zum Anfordern eines CA-Zertifikats in einer Hierarchie

Befolgen Sie die nachfolgend beschriebenen Anweisungen, um ein CA-Zertifikat mit Hilfe des Hierarchiemodells anzufordern:

1. Führen Sie im Namen des anfordernden CA folgende Schritte gemäß den Anweisungen zur web-gestützten Registrierung im *Tivoli PKI Benutzerhandbuch* aus:

   a. Führen Sie eine Vorabregistrierung aus und geben Sie an, dass die Anforderung für einen CA erfolgt.

      Achten Sie beim Ausfüllen des Registrierungsformulars darauf, einen registrierten Namen (DN) einzugeben, der mit dem des anfordernden CA übereinstimmt.

   b. Prüfen Sie den Status der Registrierungsanforderung.

   c. Befolgen Sie die Anweisung am Ende des Abschnitts, um die Vorabregistrierungsdatei zu speichern.

2. Übertragen Sie die Vorabregistrierungsdatei auf die Maschine, auf der sich der anfordernde CA der Hierarchie befindet.

3. Melden Sie sich bei Tivoli PKI als der Benutzer an, der das System auf der Maschine installiert hat, auf der sich der anfordernde CA befindet.

4. Führen Sie den Befehl **CACertRq** aus, und zwar unter AIX über die Befehlszeile und unter Windows NT über die DOS-Eingabeaufforderung.

   Stellen Sie bei Ausführung des Befehls **CACertRq** sicher, dass Sie den absoluten Pfad und den Namen der Vorabregistrierungsdatei eingeben. Informationen zur Befehlssyntax und Parameterbeschreibungen finden Sie im Abschnitt „Dienstprogramm CA Certification” auf Seite 112.

   Anmerkung: Wenn Sie als Parameter eines Befehls einen Verzeichnispfad angeben, der eingebettete Leerzeichen enthält, müssen Sie den Pfad in doppelte Anführungszeichen (″ ″) setzen. Für den Befehl **CACertRq** beispielsweise würden Sie den Parameter ’-r’ *vorabregistrierungspfad* (mit eingebetteten Leerzeichen) folgendermaßen angeben:

   ```
   CACertRq -d .companyA.com -h -r "c:\Program Files\IBM
   \Trust Authority\ccprereg.reg" -P 1835 -W Secure99
   ```

IP-Adressmaske angeben

Sie können ein gegenseitig zertifiziertes CA-Zertifikat anfordern, das die CA-Hierarchie eines anderen CA übernimmt und die Gültigkeit des Zertifikats auf die IP-Adressen einschränkt, die von Ihrem Unternehmen verwendet werden.

Im folgenden Beispiel ist das Betriebssystem AIX, Ihr Unternehmen verwendet IP-Adressen im Bereich von 9.0.0.0. bis 9.255.255.254, die Vorabregistrierungsdatei befindet sich im Pfad /tmp/ccprereg.reg, und das Kennwort lautet Secure99. Folgender Befehl platziert den angegebenen Adressenbereich in der Liste zulässiger Unterverzeichnisstrukturen:

```
CACertRq -i 9.0.0.0/255.0.0.0 -h -r  /tmp/ccprereg.reg -P 1835 -W Secure99
```

DNS-Adressen angeben

Sie können ein CA-Zertifikat anfordern, das die CA-Hierarchie eines anderen CA übernimmt und die Gültigkeit des Zertifikats auf eine Gruppe von DNS-Adressen einschränkt.

Im folgenden Beispiel wird das Betriebssystem Windows NT verwendet, alle Tivoli PKI-CA-Hosts verfügen über DNS-Adressen, die mit .companyA.com enden, Pfad und Dateiname der

Vorabregistrierungsdatei lauten a:\ccprereg.reg, und das Kennwort lautet Secure99. Mit folgendem Befehl werden die angegebenen DNS-Adressen in der Liste der zulässigen Unterverzeichnisstrukturen platziert:

```
CACertRq -d .companyA.com -h -r a:\ccprereg.reg -P 1835 -W Secure99
```

Anmerkung: Beginnt eine DNS-Adresse mit einem Punkt, werden alle Hosts einbezogen, die mit dieser Unterzeichenfolge (einschließlich '.') enden. Diese Adressen werden in die Liste der Unterverzeichnisstrukturen aufgenommen. Beginnt die Adresse nicht mit einem Punkt, wird nur der Host einbezogen, dessen Name der Zeichenfolge entspricht.

Der Einschränkung '.companyA.com' entsprechen beispielsweise us.companyA.com, vnet.companyA.com und w3.software.companyA.com, jedoch nicht companyA.com (oder kidcompanyA.com) selbst. Der Einschränkung companyA.com entsprechen companyA.com, jedoch nicht us.companyA.com oder die übrigen Adressen. Daraus folgt, dass eine zulässige Unterverzeichnisstrukturen ohne führenden Punkt '.″ nur einen möglichen Knoten angibt. Angaben ohne einen führenden Punkt werden primär für nicht zulässige Unterverzeichnisstrukturen verwendet.

E-Mail-Adressen angeben

Sie können ein CA-Zertifikat anfordern, das die CA-Hierarchie eines anderen CA übernimmt und die Gültigkeit des Zertifikats auf eine Gruppe von E-Mail-Adressen einschränkt.

Im folgenden Beispiel wird das Betriebssystem AIX verwendet, alle Tivoli PKI-CA-Hosts verfügen über E-Mail-Adressen, die mit .us.companyA.com enden, Pfad und Dateiname der Vorabregistrierungsdatei lauten /tmp/ccprereg.reg, und das Kennwort lautet Secure99. Folgender Befehl platziert die angegebenen E-Mail-Adressen in der Liste zulässiger Unterverzeichnisstrukturen:

```
CACertRq -m .us.companyA.com -h -r /tmp/ccprereg.reg -P 1835 -W Secure99
```

Sie können ein CA-Zertifikat anfordern, das die CA-Hierarchie eines anderen CA übernimmt und die Gültigkeit des Zertifikats auf alle bis auf ein Element einer Gruppe von E-Mail-Adressen einschränkt. Im folgenden Beispiel hat der Tivoli PKI-CA-Host die E-Mail-Adresse outCA.us.companyA.com, Pfad und Dateiname der Vorabregistrierungsdatei lauten '/tmp/ccprereg.reg', und das Kennwort lautet 'Secure99'. Folgender Befehl platziert die angegebene E-Mail-Adresse in der Liste nicht zulässiger Unterverzeichnisstrukturen:

```
CACertRq -m .us.companyA.com -M outCA.us.companyA.com -h -r /tmp/ccprereg.reg -P 1835
   Secure99
```

URIs angeben

Sie können ein CA-Zertifikat anfordern, das die CA-Hierarchie eines anderen CA übernimmt und die Gültigkeit des Zertifikats auf eine Gruppe von URIs (Uniform Resource Identifiers, eine Kennungskategorie, die hauptsächlich aus URL-Adressen besteht) einschränkt. Im folgenden Beispiel wird das Betriebssystem Windows NT verwendet, alle Tivoli PKI-CA-Hosts verfügen über URIs, die mit .xyz.com enden, Pfad und Dateiname der Vorabregistrierungsdatei lauten 'a:\ccprereg.reg', und das Kennwort lautet 'Secure99'. Folgender Befehl platziert die angegebene URI in der Liste zulässiger Unterverzeichnisstrukturen:

```
CACertRq -u .xyz.com -h -r a:\ccprereg.reg -P 1835 -W Secure99
```

Anmerkung: Der Knotenabschnitt der URI unterliegt den im Abschnitt „DNS-Adressen angeben" auf Seite 23 beschriebenen Regeln, sofern er keine IP-Adressen enthält. In diesem Fall wird er als exakte Übereinstimmung behandelt.

Verzeichniseinträge angeben

Sie können ein CA-Zertifikat anfordern, das die CA-Hierarchie eines anderen CA übernimmt und die Gültigkeit des Zertifikats auf eine Gruppe von Verzeichniseinträgen mit den gleichen RDNs (Relative Distinguished Names, relative registrierte Namen) einschränkt. Im folgenden Beispiel wird das Betriebssystem AIX verwendet, alle Tivoli PKI-CA-Hosts verfügen über RDNs, die den angegebenen RDNs (/C=US/O=companyA/OU=departmentB) entsprechen, Pfad und Dateiname der Vorabregistrierungsdatei lauten '/tmp/ccprereg.reg', und das Kennwort lautet 'Secure99'. Folgender Befehl platziert den angegebenen RDN in der Liste der zulässigen Unterverzeichnisstrukturen:

```
CACertRq -n "/C=US/O=companyA/OU=departmentB" -h -r /tmp/ccprereg.reg -P 1835 -W Secure99
```

Anmerkung: In Tivoli PKI wird für DNs folgendes Format verwendet:

```
/C=Land/O=Unternehmen/OU=Unternehmenseinheit/CN=allgemeiner_Name
```

Namenseinschränkungen ausschließen

Wenn Sie planen, als Teil Ihrer allgemeinen Hierarchielösung die hierarchischen CA-Zertifikate in Netscape Communicator herunterzuladen, sollten Sie den Parameter '-m ..' mit dem Dienstprogramm 'CA Certification' verwenden, um die Erweiterung für Namenseinschränkungen (Name Constraints) aus dem resultierenden CA-Zertifikat auszuschließen. Im folgenden Beispiel wird das Betriebssystem Windows NT ausgeführt, und es werden jeweils die Standardwerte für den Installationspfad, den Namen der Vorabregistrierungsdatei und das Systemkennwort von Tivoli PKI verwendet. Das Exemplar eines solchen Befehls könnte beispielsweise folgendermaßen aussehen:

```
CACertRq -m .. -h -r "c:\Program Files\IBM\Trust Authority\ccprereg.reg" -P 1835 -W Secure99
```

CA-Zertifikat von Fremd-CA erhalten

Mit Tivoli PKI können Sie ein CA-Zertifikat von einem Fremd-CA empfangen. Indem Sie das Zertifikat dieses Fremd-CA akzeptieren, ordnen Sie anschließend den Tivoli PKI-CA dem Fremd-CA hierarchisch unter. So können Sie ein CA-Zertifikat von einem Fremd-CA empfangen:

1. Erstellen Sie eine PKCS#10-Anforderungsdatei. Verwenden Sie hierzu das Dienstprogramm CA Certification (CACertRq). Die Anforderung kann entweder im Binärformat oder im Base-64-Format erstellt werden. Führen Sie den Befehl **CACertRq** mit dem Parameter '-P' aus, nach dem Sie die Nummer des Verwaltungs-Ports für den CA angeben. Verwenden Sie außerdem den Parameter '-C', um die Anforderungsdatei im Binärformat zu erstellen, oder den Parameter '-B', damit die Anforderungsdatei im Base-64-Format erstellt wird. Die Anforderungsdatei muss über eine sichere, im Offlinemodus verwendete Methode Ihrer Wahl an den Fremd-CA übertragen werden. Während der Übertragung müssen Sie und der Fremd-CA, der die Datei empfängt, dafür sorgen, dass Sicherheit und Integrität dieser Datei gewährleistet sind.
2. Der Fremd-CA nimmt die Anforderungsdatei an und gibt dann eine Antwortdatei an Sie zurück. Die Antwortdatei muss im Binärformat stehen und eine codierte PKCS#7-Kette von CA-Zertifikaten enthalten, einschließlich des an Ihren Tivoli PKI-CA ausgestellten Zertifikats und des Zertifikats für den CA auf der Ausgangsebene der Hierarchie. Die Antwortdatei muss vom Fremd-CA über eine sichere, im Offlinemodus verwendete Methode Ihrer Wahl übertragen werden. Während der Übertragung müssen Sie und der Fremd-CA dafür sorgen, dass Sicherheit und Integrität der Antwortdatei gewährleistet

sind. Speichern Sie die Antwortdatei in einem beliebigen Verzeichnis, und stellen Sie sicher, dass das Benutzerkonto 'cfguser' zum Lesezugriff auf die Datei berechtigt ist.

3. Führen Sie das Dienstprogramm CA Certification aus, um die Antwortdatei vom Fremd-CA zu verarbeiten. Führen Sie den Befehl **CACertRq** mit dem Parameter '-P' aus, nach dem Sie die Nummer des Verwaltungs-Ports für den CA angeben. Verwenden Sie außerdem den Parameter '-S', gefolgt vom vollständigen Pfad der Antwortdatei. Mit diesem Schritt werden außerdem die Dateien 'CAChain.p7b', 'CAChain.b64', 'RAsCopyOfCAChain.p7b' und 'RAsCopyOfCAChain.b64' aktualisiert.

Aktualisierungen nach Änderung der CA-Hierarchie vornehmen

Immer dann, wenn Sie den Unterzeichner Ihrer Zertifikate ändern, indem Sie entweder die interne oder die übergeordnete Hierarchie ändern, müssen Sie diese Änderungen für jede einzelne RA anlegen. Beim Ändern der Hierarchie wird die neue Hierarchiestruktur in die Dateien 'CAChain.p7b', 'RAsCopyOfCAChain.p7b', 'CAChain.b64' und 'RAsCopyOfCAChain.b64' geschrieben. Die Dateien 'CAChain.*xxx*' können sofort verwendet werden. Die neuen Dateien 'RAsCopyOfCAChain.*xxx*' müssen jedoch zunächst an alle RAs übertragen werden, die unter diesem CA ausgeführt werden. Die neuen Dateien 'RAsCopyOfCAChain.*xxx*' müssen an die RAs mit einer sicheren, im Offlinemodus verwendeten Methode Ihrer Wahl übertragen werden. Während der Übertragung müssen Sie dafür sorgen, dass Sicherheit und Integrität dieser Dateien gewährleistet sind. Sobald die alten Versionen der Dateien 'RAsCopyOfCAChain.*xxx*' auf jedem RA-System ersetzt wurden, das unter dem CA mit der geänderten Hierarchie ausgeführt wird, akzeptieren alle ausgestellten Zertifikate die neue Hierarchie und können wie gewohnt verwendet werden.

Anmerkung: Sollte ein Benutzer versuchen, in dem Zeitraum zwischen der Änderung der Hierarchie und der Aktualisierung der Dateien 'RasCopyOfCAChain.*xxx*' auf den einzelnen RAs ein Zertifikat zu verwenden, schlägt die Authentifizierung des Zertifikats fehl. Daher ist es wichtig, diesen Zeitraum so kurz wie möglich zu halten.

Schlüsselbund des Webservers nach Aufbau der CA-Hierarchie aktualisieren

Nachdem Sie eine CA-Hierarchie aufgebaut haben, in der der Tivoli PKI-CA der ausstellende CA ist (also das Tivoli PKI-CA-Zertifikat durch einen anderen CA unterzeichnet wurde), müssen Sie den Schlüsselbund des Webservers auf dem Tivoli PKI-System aktualisieren, damit diese neue Hierarchie wiedergegeben wird. So aktualisieren Sie den Schlüsselbund des Webservers:

1. Geben Sie auf der RA-Maschine Folgendes in der Befehlszeile ein:
   ```
   gsk4ikm
   ```
2. Wählen Sie **Key Database File** und dann **Open** aus.
3. Geben Sie den Pfad- bzw. Ordnernamen für den Schlüsselspeicher des Webservers ein:
   ```
   /usr/lpp/iau/etc
   ```
4. Klicken Sie auf **Update**.
5. Wählen Sie die Datei **httpd-RD.kdb** aus, und klicken Sie anschließend auf **OK**.
6. Geben Sie in der Eingabeaufforderung für das Kennwort das Kennwort für das Steuerprogramm ein. Dies ist das Kennwort, das Sie bei der Ausführung von 'CfgPostInstall' angegeben haben.

Anmerkung: Falls Sie nach der Konfiguration von Tivoli PKI das Kennwort für das Steuerprogramm ändern, wird das Schlüsselbundkennwort des Webservers für die Datei '/usr/lpp/iau/etc/httpd-RD.kdb' nicht geändert. Dieses Kennwort bleibt mit dem ursprünglichen Kennwort für das Steuerprogramm identisch.

7. Klicken Sie auf **OK**.
8. Klicken Sie unter **Key database content** auf das Dropdown-Menü, und wählen Sie die Option **Signer Certificates** aus.
9. Wählen Sie das Unterzeichnerzertifikat mit der Bezeichnung **Trust Authority** aus, und klicken Sie dann auf **Delete**.
10. Verlassen Sie das Schlüsselbundprogramm 'gsk4ikm'.
11. Wechseln Sie auf der RA-Maschine zum Benutzerkonto 'cfguser', indem Sie den folgenden Befehl eingeben:

    ```
    su - cfguser
    ```

12. Geben Sie Folgendes ein, um das Verzeichnis zu wechseln:

    ```
    cd /usr/lpp/iau/bin
    ```

13. Geben Sie den folgenden Befehl ein, und setzen Sie hierbei die entsprechenden Werte ein:

    ```
    ./kdbUtils -i -m 3 -f /usr/lpp/iau/etc/httpd-RD.kdb -r
       /usr/lpp/iau/etc/RAsCopyOfCAChain.b64  -p kennwort -l kennung -L protokolldatei
    ```

    Hierbei gilt:

    kennwort
    : Das ursprüngliche Kennwort für das Steuerprogramm, dass Sie bei 'CfgPostInstall' eingegeben haben.

    kennung
    : Die Kennung, die Sie für das CA-Zertifikat bzw. die CA-Zertifikate vergeben wollen, das/die Sie importieren.

    protokolldatei
    : Die Protokolldatei für diesen Befehl. Sie müssen sicherstellen, dass das Benutzerkonto 'cfguser' für den Schreibzugriff auf das Verzeichnis berechtigt ist, in dem die Protokolldatei erstellt wird.

14. Stoppen Sie Tivoli PKI.
15. Starten Sie Tivoli PKI.

CA-Schlüssel aktualisieren

Mit dem Dienstprogramm CA Key Update können Sie eine Schlüsselaktualisierung oder einen *Rollover-Prozess* aus einem unbeschädigten CA-Schlüsselpaar auf das nächste CA-Schlüsselpaar einleiten. Sobald die Erstellung vorgenommen wurde, verwendet der CA beim Unterzeichnen von Zertifikaten das neue Schlüsselpaar. Nach Ausführung eines CA-Key-Rollover-Prozesses müssen Sie das Webserverzertifikat aktualisieren, damit der neue CA-Unterschriftsschlüssel verwendet wird.

Weitere Details und Referenzinformationen finden Sie im Abschnitt „Dienstprogramm CA Key Update" auf Seite 124.

So können Sie eine CA-Schlüsselaktualisierung vornehmen und das Webserverzertifikat aktualisieren:

1. Stoppen Sie das Tivoli PKI-System. Lesen Sie gegebenenfalls die Anweisungen unter „Serverkomponenten starten und stoppen” auf Seite 8 nach.
2. Melden Sie sich am CA-Server als **cfguser** an, und geben Sie Folgendes ein, um das Verzeichnis zu wechseln:

   ```
   /usr/lpp/iau/bin
   ```

3. Geben Sie Folgendes ein, um die CA-Schlüsselaktualisierung zu starten:

   ```
   ./cakeyroll
   ```

   Nach Beendigung des Befehls wird die folgende Nachricht angezeigt:

   ```
   CA-Key-Rollover wurde gestartet. Sie können nun den Befehl Start_TA.sh
   eingeben.
   ```

4. Geben Sie den folgenden Befehl ein:

   ```
   ./Start_TA.sh
   ```

5. Überprüfen Sie nach Absetzen des Befehls **Start_TA.sh**, ob die CA-Protokolldatei die folgende Nachricht enthält:

   ```
   Ausführung von CA-Key-Rollover für
   RA ra-name erfolgreich.
   ```

   Hierbei steht *ra-name* für den Namen Ihrer RA.

   Anmerkung: Wenn Sie mehrere RAs verwenden, sollte diese Nachricht für jede RA ausgegeben werden.

   Stellen Sie sicher, dass das System keine Zertifikatoperationen (Registrierung, Widerruf, Sicherung, Wiederherstellung usw.) verarbeitet, bis diese Nachricht in der CA-Protokolldatei angezeigt wird.

6. Falls sich die RA und der CA auf unterschiedlichen Maschinen befinden, kopieren Sie die folgenden Dateien auf jede RA:
   - caCertificate
   - RAsCopyOfCAChain.b64
   - RAsCopyOfCAChain.p7b

   In der Standardeinstellung befinden sich diese Dateien auf dem CA und der RA im Verzeichnis ’/usr/lpp/iau/etc’.

7. Geben Sie auf der RA-Maschine Folgendes in der Befehlszeile ein, um das Verzeichnis zu wechseln:

   ```
   cd  /usr/opt/ibm/gskit/bin
   ```

8. Geben Sie den folgenden Befehl ein, um die GUI für die Schlüsselverwaltung (Key Management GUI) zu aktivieren:

   ```
   ./gsk4ikm
   ```

9. Wählen Sie **Key Database File** und dann **Open** aus.
10. Geben Sie den Pfad- bzw. Ordnernamen für den Schlüsselspeicher des Webservers ein:

    ```
    /usr/lpp/iau/etc
    ```

11. Klicken Sie auf **Update**.

12. Wählen Sie die Datei **httpd-RD.kdb** aus, und klicken Sie anschließend auf **OK**.
13. Geben Sie in der Eingabeaufforderung für das Kennwort das Kennwort für das Steuerprogramm ein. Dies ist das Kennwort, das Sie bei der Ausführung von 'CfgPostInstall' angegeben haben.

    Anmerkung: Falls Sie nach der Konfiguration von Tivoli PKI das Kennwort für das Steuerprogramm ändern, wird das Schlüsselbundkennwort des Webservers für die Datei '/usr/lpp/iau/etc/httpd-RA.kdb' nicht geändert.
14. Klicken Sie auf **OK**.
15. Klicken Sie unter **Key database content** auf das Dropdown-Menü, und wählen Sie die Option **Personal Certificate Requests** aus.
16. Klicken Sie auf **New**, um ein neues Zertifikat anzufordern.
17. Geben Sie die entsprechenden Werte für die Felder in der Anzeige **Create New Key and Certificate Request** an. Die anzugebenden Werte sind mit den Werten identisch, die Sie während der Konfiguration von Tivoli PKI angegeben haben. Der Wert, den Sie für **Key Label** angeben, wird an einer späteren Stelle in dieser Prozedur verwendet.
18. Nachdem Sie die erforderlichen Informationen eingegeben haben, geben Sie den Namen der Datei an, in der die Zertifikatsanforderung gespeichert werden soll.
19. Klicken Sie auf **OK**. Es wird die Nachricht ausgegeben, dass die Operation erfolgreich abgeschlossen wurde.
20. Klicken Sie auf **OK**. Die Datei wird jetzt unter **Personal Certificate Requests** aufgeführt.
21. Editieren Sie die in Schritt 18 erstellte Datei mit einem Texteditor, und kopieren Sie den Inhalt der PKCS#10-Datei in die Zwischenablage.
22. Rufen Sie in Ihrem Browser die Tivoli PKI-Seite **index.jsp** auf.
23. Setzen Sie eine Anforderung für ein neues Server- oder Einheitenzertifikat ab. Ausführliche Angaben hierzu finden Sie im *Tivoli PKI Benutzerhandbuch*.
24. Nachdem Sie die entsprechenden Anforderungsinformationen angegeben haben, fügen Sie die PKCS#10-Informationen aus Schritt 21 in das Feld **PKCS#10-Zertifikatsanforderung** ein.
25. Klicken Sie auf **Registrierungsanforderung übergeben**.
26. Bestätigen Sie die Zertifikatsanforderung am RA Desktop. Ausführliche Angaben hierzu finden Sie im Handbuch *Tivoli PKI RA Desktop*.
27. Klicken Sie in dem Browser, über den Sie das Serverzertifikat angefordert, auf **Registrierungsstatus überprüfen**, um die PKCS#7-Datei abzurufen.
28. Wählen Sie für **Format der Zertifikatsdatei** die Einstellung **Base64-verschlüsseltes PKCS#7-Zertifikat für PC (CRLF)** aus.
29. Klicken Sie auf **Zertifikat auf Platte sichern**, und geben Sie an, in welcher Position die Datei gespeichert werden soll.
30. Übertragen Sie die in Schritt 29 gespeicherte Zertifikatsdatei per E-Mail oder mittels einer anderen Methode an die RA-Maschine.

31. Wechseln Sie auf der RA-Maschine zum Benutzerkonto 'cfguser', indem Sie den folgenden Befehl eingeben:

    ```
    su - cfguser
    ```

32. Geben Sie Folgendes ein, um das Verzeichnis zu wechseln:

    ```
    cd /usr/lpp/iau/bin
    ```

33. Geben Sie den folgenden Befehl ein, und setzen Sie hierbei die entsprechenden Werte ein:

    ```
    ./kdbUtils -i -m 3 -f /usr/lpp/iau/etc/httpd-RD.kdb -r
       /usr/lpp/iau/etc/RAsCopyOfCAChain.b64  -p kennwort -l kennung -L protokolldatei
    ```

    Hierbei gilt:

    kennwort
    : Das ursprüngliche Kennwort für das Steuerprogramm, dass Sie bei 'CfgPostInstall' eingegeben haben.

    kennung
    : Die Kennung, die Sie für das CA-Zertifikat bzw. die CA-Zertifikate vergeben wollen, das/die Sie importieren.

    protokolldatei
    : Die Protokolldatei für diesen Befehl. Sie müssen sicherstellen, dass das Benutzerkonto 'cfguser' zum Schreibzugriff auf das Verzeichnis berechtigt ist, in dem die Protokolldatei erstellt wird.

34. Verwenden Sie auf der RA-Maschine die GUI für die Schlüsselverwaltung (Key Management GUI), und wechseln Sie zu **Personal Certificates**.
35. Klicken Sie auf **Receive**. Die Anzeige **Receive from a File** wird aufgerufen.
36. Geben Sie den Namen der PKCS#7-Zertifikatsdatei an, die Sie in Schritt 29 auf Seite 32 gespeichert haben.
37. Geben Sie die Pfadinformationen für die Zertifikatsdatei an, die Sie in Schritt 30 auf Seite 32 gespeichert haben.
38. Klicken Sie auf **OK**.
39. Geben Sie die entsprechende Antwort, sobald mit der folgenden Nachricht angefragt wird, ob der Schlüssel in der Datenbank als Standardschlüssel definiert werden soll:

    ```
    Do you want to set the key as the default key in the
    database?
    ```

40. Schließen Sie die GUI für die Schlüsselverwaltung.
41. Geben Sie Folgendes ein, um das Verzeichnis zu wechseln:

    ```
    cd /usr/lpp/iau/pkrf/Domains/[ihre_domäne]/
    ```

42. Öffnen Sie die Datei 'httpd-RD_0.conf' in einem Texteditor.
43. Suchen Sie nach allen Exemplaren von SSLServerCert, und ersetzen Sie diese durch die **Schlüsselkennung**, die Sie in Schritt 17 auf Seite 32 angegeben haben. Diese Datei enthält zwei Exemplare von SSLServerCert.
44. Speichern Sie die Datei, und beenden Sie die Datei.
45. Stoppen Sie Tivoli PKI.
46. Starten Sie Tivoli PKI.

CA-Serverprotokolle prüfen

Die Protokolle des CA-Servers zeichnen alle Transaktionen mit dem CA-Server auf. Sie können die Protokolle des CA-Servers in der nachfolgend beschriebenen Position prüfen:

Tabelle 4. Protokolle des CA-Servers

AIX-Standardpfad	Windows NT-Standardpfad	Beschreibung
/usr/lpp/iau/etc/TrustAuthority	c:\Program Files\IBM\Trust Authority\etc\TrustAuthority	Für Protokolldateinamen gilt der Stamm caSS.log. Für jede neue Protokolldatei wird die Erweiterung *xnnnnnn* inkrementell erhöht.

CA-Serverstatus prüfen

Je nach Umgebung können Sie den Status des CA-Servers mit folgenden Prozeduren prüfen:

- Unter AIX:
  1. Melden Sie sich bei AIX als Root an.
  2. Prüfen Sie die Prozesstabellen und suchen Sie nach folgender Zeichenfolge:
     ```
     irgAutoCa
     ```
     Finden Sie diesen Prozess, fahren Sie mit Schritt 3 fort. Finden Sie diesen Prozess nicht, lesen Sie bitte im Abschnitt „Fehlerbehebung” auf Seite 135 nach.
  3. Wechseln Sie in das Verzeichnis 'bin'. Dieses Verzeichnis hat folgenden Standardpfad:
     ```
     /usr/lpp/iau/bin
     ```
  4. Prüfen Sie, ob Port 1835 erfolgreich antwortet, indem Sie folgenden Befehl eingeben:
     ServerControl -i -c -k CA -n *Server* **-p 1835 -l "***Protokolldatei***"**

     Hierbei steht *Server* für den Namen des CA-Servers, der dem Port 1835 zugeordnet ist, und *Protokolldatei* für den Namen der Datei, in der die Ergebnisse des Befehls **ServerControl** aufgezeichnet werden sollen.

     Ist die Antwort des geprüften Ports erfolgreich, wird folgende Nachricht angezeigt:
     ```
     Es wurde
     festgestellt, dass der [CA]-Service auf dem Server an Port 1835 ausgeführt wird.
     ```
     Hierbei steht *Server* für den Server, der dem Port 1835 zugeordnet ist.
- Unter Windows NT:
  1. Melden Sie sich bei Windows NT als Systemadministrator an.
  2. Starten Sie den Task-Manager durch Drücken der Tastenkombination **Strg**, **Alt** und **Entf**.
  3. Wählen Sie die Registerkarte **Prozesse** aus.
  4. Suchen Sie nach dem Prozess irgAutoCA.exe.

     Finden Sie diesen Prozess, fahren Sie mit Schritt 5 auf Seite 35 fort. Finden Sie diesen Prozess nicht, lesen Sie bitte im Abschnitt „Fehlerbehebung” auf Seite 135 nach.

5. Wechseln Sie an der MS DOS-Eingabeaufforderung in das Verzeichnis 'bin'. Dieses Verzeichnis hat folgenden Standardpfad:

   ```
   c:\Program Files\IBM\Trust Authority\bin
   ```

6. Prüfen Sie, ob Port 1835 erfolgreich antwortet, indem Sie folgenden Befehl eingeben:

   ServerControl -i -c -k CA -n *Server* **-p 1835 -l "***Protokolldatei***"**

   Hierbei steht *Server* für den Namen des CA-Servers, der dem Port 1835 zugeordnet ist, und *Protokolldatei* für den Namen der Datei, in der die Ergebnisse des Befehls **ServerControl** aufgezeichnet werden sollen.

   Ist die Antwort des geprüften Ports erfolgreich, wird folgende Nachricht angezeigt:

   ```
   Es wurde
   festgestellt, dass der [CA]-Service auf dem
   Server an Port 1835 ausgeführt wird.
   ```

   Hierbei steht *Server* für den Server, der dem Port 1835 zugeordnet ist.

CRL-Verteilungspunkte aktivieren

So können Sie die CRL-Verteilungspunkte aktivieren:

1. Melden Sie sich bei Ihrem Betriebssystem als Administrator an.
2. Stoppen Sie das Tivoli PKI-System.
3. Laden Sie die Konfigurationsdatei 'jonahca.ini' in einen Texteditor. Informationen zu den Dateipositionen unter AIX und Windows NT finden Sie in Tabelle 12 auf Seite 84.
4. Editieren Sie im Abschnitt **General** den Parameter **CertperDP**.
5. Ändern Sie den Wert in eine positive ganze Zahl ungleich Null.
6. Editieren Sie im Abschnitt **General** den Parameter **CRLDistName**.
7. Ändern Sie den Wert in einen aussagekräftigen Namen. Die Zeichen **%d** im Namen müssen beibehalten werden.
8. Speichern Sie die Datei.
9. Starten Sie das Tivoli PKI-System.

RA-Server verwalten

In diesem Abschnitt werden Prozeduren für Betrieb und Verwaltung des Tivoli PKI Registrierungsstellen-Servers (RA-Server) erläutert. Der RA-Server verwaltet die Kommunikation zwischen RA Desktop und CA-Server. Er befindet sich zusammen mit seinem DB2-Datenbankexemplar auf einer lokalen Maschine.

Die folgenden Tasks zur Verwaltung des CA-Servers werden beschrieben:

- Verwendung des Dienstprogramms Add RA User (add_rauser), um Benutzer zum System als Registrator (RA-Administratoren) hinzuzufügen
- Verwendung des Dienstprogramms Enable RA Database Encryption (iauEnableRADBSec), um die Verschlüsselung der RA-Datenbank zu aktivieren

- Vornahme der folgenden Änderungen an der Konfigurationsdatei 'jonahra.ini' mit einem Texteditor:
  - Änderung des Listener-Ports für den RA-Server
  - Ändern des RA-Sendeaufrufintervalls
  - Ändern des RA-Wiederholungsintervalls
  - Ändern der RA-Einstellungen für die Kommunikation mit dem Directory
- Prüfen der RA-Serverprotokolle
- Prüfen des Status des RA-Servers

Registratoren hinzufügen

Sie sind für das Hinzufügen neuer Registratoren zum System verantwortlich. Ein Benutzer mit dem Status eines Registrators kann die Funktionen nutzen und auf die eingeschränkten Ressourcen zugreifen, die in einem der RA-Profile in der Konfigurationsdatei einer Tivoli PKI-Registrierungseinrichtung definiert wurden. Um einen neuen Registrator hinzufügen zu können, müssen Sie selbst ein RA-Administrator sein. Dieser Abschnitt erläutert die Prozeduren zum erstmaligen Anfordern des Identitätsnachweises als RA-Administrator und zum Hinzufügen eines weiteren RA-Administrators.

Eigenes Benutzerkonto als ersten Registrator hinzufügen

So fügen Sie sich selbst dem Tivoli PKI-System als Registrator hinzu:

1. Fordern Sie ein Browser-Zertifikat an, sofern Sie noch keines besitzen. Fahren Sie fort, wenn Sie dieses Zertifikat erhalten haben. Entsprechende Anweisungen finden Sie im Handbuch *Tivoli PKI Benutzerhandbuch*.
2. Tragen Sie einen der folgenden Identifikationscodes ein:
   - Die Anforderungs-ID, die während der Browser-Registrierung für Sie generiert wurde.

     Wenn Sie sich erst kürzlich für ein Browser-Zertifikat registriert haben, verfügen Sie möglicherweise noch über diese ID.
   - Die Identitätsnachweis-UUID (eindeutige Benutzer-ID), die aufgrund der erfolgreichen Browser-Registrierung generiert wurde.

     So können Sie Ihre Identitätsnachweis-UUID erhalten:

     a. Starten Sie eine interaktive DB2-Befehlszeilensitzung. Verwenden Sie je nach Betriebssystem folgende Prozeduren:
        - Unter AIX:
          1) Geben Sie an der Eingabeaufforderung den Befehl **su** ein, um zum Konto des Benutzers mit Administratorberechtigung zu wechseln, der Tivoli PKI installiert hat.
          2) Geben Sie das Kennwort dieses Tivoli PKI-Benutzers ein.
          3) Geben Sie den Befehl **db2** ein, um die DB2-Sitzung zu starten.
          4) Geben Sie an der Eingabeaufforderung folgenden Befehl ein, um die Verbindung zur Datenbank herzustellen:

             ```
             connect to pkrfdb
             ```

             In diesem Beispiel wird die Standard-Registrierungsdatenbank 'pkrfdb' verwendet.

- Unter Windows NT:

  1) Wählen Sie in der Windows-Funktionsleiste die Option **Start → Programme → DB2 für Windows NT → Befehlszeilenprozessor** aus.

  2) Geben Sie an der Eingabeaufforderung den Befehl **DB2** ein.

  3) Geben Sie an der Eingabeaufforderung folgenden Befehl ein, um die Verbindung zur Datenbank herzustellen:

     ```
     connect to pkrfdb
     ```

     In diesem Beispiel wird die Standard-Registrierungsdatenbank 'pkrfdb' verwendet.

b. Geben Sie an der DB2-Eingabeaufforderung einen SQL-Befehl nach folgendem Muster ein:

```
select last_name, first_name, credential_uuid, created_on from requests
   where last_name = 'IhrNachname' and first_name =
'IhrVorname' and
   profile_name like '%BrowserCert%'
```

Ist diese Abfrage erfolgreich, gibt das System den angeforderten Nachnamen, Vornamen, die Identitätsnachweis-UUID und die Zeitmarke aller entsprechenden Einträge zurück. In diesem Beispiel handelt es sich bei den zurückgegebenen Informationen um Angaben aus dem Anforderungssatz Ihres genehmigten Browser-Zertifikats.

c. Geben Sie den Befehl **quit** ein, um die DB2-Sitzung zu beenden.

3. Befolgen Sie die Anweisungen im Abschnitt „Registrator hinzufügen" ab Schritt 3 auf Seite 38, um das Hinzufügen des eigenen Benutzerkontos als ersten Registrator abzuschließen.

Registrator hinzufügen

Je nach den von Ihrem Unternehmen festgelegten Regeln kann eine Anforderung zum Hinzufügen eines Registrators auf verschiedene Weise gestellt werden, beispielsweise in Form eines informellen Telefongesprächs oder über einen formellen Antragsprozess. Um als Registrator berechtigt werden zu können, muss der betreffende Benutzer in den meisten Unternehmen zunächst ein SSL-Browser-Zertifikat erhalten. Benutzer können Browser-Zertifikate anfordern, indem Sie die browser-gestützten Standardregistrierungsanweisungen im *Tivoli PKI Benutzerhandbuch* befolgen.

Tivoli PKI bietet zum Hinzufügen von Registratoren das Befehlszeilendienstprogramm 'add_rauser'. Die Syntax dieses Befehls wird im Abschnitt „Dienstprogramm Add RA User" auf Seite 115 erläutert.

So können Sie nach Erhalt einer Anforderung dem System einen Registrator hinzufügen:

1. Prüfen Sie den Status der Anforderung des SSL-Browser-Zertifikats des zukünftigen Registrators.

   Greifen Sie hierzu auf RA Desktop zu, und befolgen Sie die im Handbuch *Tivoli PKI Registration Authority Desktop* dokumentierten Prozeduren, um eine Abfrage zu übergeben und die Ergebnisse anzuzeigen.

2. Wurde ein Zertifikat ausgestellt, notieren Sie die ihm zugeordnete Identitätsnachweis-UUID.

Anmerkung: Sie können auch die Anforderungs-ID verwenden, die während einer erfolgreichen Browser-Registrierung für ein Zertifikat generiert wurde.

Um die Identitätsnachweis-UUID zu erhalten, lokalisieren Sie den Datenbankeintrag für das genehmigte Zertifikat, und zeigen Sie die Attribute dieses Eintrags an. Sie benötigen das Attribut der Identitätsnachweis-UUID, das Sie als einen Parameter des Befehls 'add_rauser' verwenden müssen.

3. Führen Sie je nach Umgebung einen der folgenden Schritte aus:

   - Unter AIX:

     a. Wechseln Sie in das Stammverzeichnis der Installation. Geben Sie dazu bei Verwendung des Standard-Stammverzeichnisses folgenden Befehl ein:

        ```
        cd /usr/lpp/iau/bin
        ```

     b. Geben Sie einen Befehl nach folgendem Muster ein:

        ```
        ./add_rauser /usr/lpp/iau/pkrf/etc/domain.cfg YourDomain aBcXyZ==
        ```

        Dabei gilt:

        - `/usr/lpp/iau/pkrf/etc/domain.cfg` ist der Pfad des Standardstammverzeichnisses der Tivoli PKI-Installation und der Domänenkonfigurationsdatei.
        - *YourDomain* ist die Standard-Registrierungsdomäne.
        - `aBcXyZ==` ist entweder ein Beispiel einer Anforderungs-ID oder einer Identitätsnachweis-UUID.

   - Unter Windows NT:

     a. Wechseln Sie in das Stammverzeichnis der Installation. Geben Sie dazu bei Verwendung des Standard-Stammverzeichnisses folgenden Befehl ein:

        ```
        cd "c:\Program Files\IBM\Trust Authority\bin"
        ```

     b. Geben Sie einen Befehl nach folgendem Muster ein:

        ```
        add_rauser "c:\Program Files\IBM\Trust Authority\pkrf\etc\domain.cfg"
             YourDomain aBcXyZ==
        ```

        Dabei gilt:

        - `c:\Program Files\IBM\Trust Authority\pkrf\etc\domain.cfg` ist der Pfad des Standardstammverzeichnisses der Tivoli PKI-Installation und der Domänenkonfigurationsdatei.

          Anmerkung: Wenn Sie als Parameter eines Befehls einen Verzeichnispfad angeben, der eingebettete Leerzeichen enthält, müssen Sie den Pfad in doppelte Anführungszeichen (″ ″) setzen.

        - *YourDomain* ist die Standard-Registrierungsdomäne.
        - `aBcXyZ==` ist entweder ein Beispiel einer Anforderungs-ID oder einer Identitätsnachweis-UUID.

Nach der Ausführung des Befehls wird eine Erfolgs- oder Fehlernachricht angezeigt.

Verschlüsselung für die RA-Datenbank aktivieren

Standardmäßig werden Informationen in der Registrierungseinrichtung-Datenbank nicht verschlüsselt. Nach der Konfiguration des Tivoli PKI-Systems können Sie die Datenbankverschlüsselung durch Ausführen des Programms 'iauEnableRADBSec' aktivieren. Wenn Sie 'iauEnableRADBSec' ausführen, untersucht das Programm die Datei 'raconfig.cfg', um festzustellen, ob die Datenbankverschlüsselung bereits aktiviert ist. Falls nicht, wird die Verschlüsselung vom Programm 'iauEnableRADBSec' aktiviert. Ist die Aktivierung bereits erfolgt, gibt das Programm eine Nachricht aus und wird beendet.

Das Programm 'iauEnableRADBSec' aktualisiert die RADATABASE- und afservice.RADB-Einträge in der Datei 'raconfig.cfg' mit den generierten Chiffrierschlüsseln. Anschließend werden die Werte für diese Einträge verschlüsselt und Base 64-codiert.

Anmerkung: Im Unterverzeichnis 'etc' des virtuellen Root-Installationsverzeichnisses, das für Ihre Registrierungsdomäne konfiguriert wurde (der im Setup Wizard angegebene Wert für das Root-Installationsverzeichnis), wird eine Sicherungskopie der Datei 'raconfig.cfg' erstellt. Der Name der Sicherungskopie lautet 'raconfig.cfg.ERADSBKUP'.

Verwenden Sie je nach Betriebssystem eine der folgenden Prozeduren, um die Verschlüsselung für die RA-Datenbank zu aktivieren:

- Unter AIX:
  1. Melden Sie sich als 'root' an:
     ```
     su - root
     ```
  2. Wechseln Sie in das Unterverzeichnis 'bin' Ihres Installationsverzeichnisses. In diesem Beispiel wird der folgende Standardinstallationspfad von Tivoli PKI verwendet:
     ```
     cd /usr/lpp/iau/bin
     ```
  3. Führen Sie das Programm 'iauEnableRADBSec' folgendermaßen aus. In diesem Beispiel werden der standardmäßige Registrierungsdomänenname und der standardmäßige Installationspfad von Tivoli PKI verwendet:
     ```
     ./iauEnableRADBSec -d YourDomain -r /usr/lpp/iau/
     ```
  4. Stoppen Sie Tivoli PKI.
  5. Starten Sie Tivoli PKI.
- Unter Windows NT:
  1. Melden Sie sich als Tivoli PKI-Konfigurationsbenutzer an (normalerweise 'cfguser').
  2. Wechseln Sie in das Unterverzeichnis 'bin' Ihres Installationsverzeichnisses. In diesem Beispiel wird der folgende Standardinstallationspfad von Tivoli PKI verwendet:
     ```
     cd "c:\Program Files\IBM\Trust Authority\bin"
     ```
  3. Führen Sie das Programm 'iauEnableRADBSec' folgendermaßen aus. In diesem Beispiel werden der standardmäßige Registrierungsdomänenname und der standardmäßige Installationspfad von Tivoli PKI verwendet:
     ```
     iauEnableRADBSec -d YourDomain -r "c:\Program Files\IBM\Trust Authority"
     ```

RA-Server-Listener-Port ändern

Der RA-Server-Listener-Port ist der Port, an dem die RA für PKIX-Nachrichten empfangsbereit ist. So können Sie den Wert für diesen Port ändern:

1. Melden Sie sich bei Ihrem Betriebssystem als Systemadministrator an.
2. Stoppen Sie das Tivoli PKI-System. Lesen Sie gegebenenfalls die Anweisungen unter „Serverkomponenten starten und stoppen” auf Seite 8 nach.
3. Laden Sie die Konfigurationsdatei ’jonahra.ini’ in einen Texteditor. Informationen zu den Dateipositionen unter AIX und Windows NT finden Sie in Tabelle 12 auf Seite 84.
4. Editieren Sie im Abschnitt **Transport** den Parameter **TCPPort**.
5. Ändern Sie den Wert der Port-Nummer.
6. Speichern Sie die Datei.
7. Laden Sie die Konfigurationsdatei ’jonahca.ini’ in einen Texteditor. (Diese Datei kann sich je nach vorhandener Installation auf einer lokalen oder einer fernen Maschine befinden.).
8. Editieren Sie den Abschnitt **URLs**.
9. Ändern Sie den Wert der Port-Nummer.
10. Speichern Sie die Datei, und beenden Sie das Programm.
11. Starten Sie das Tivoli PKI-System.

RA-Sendeaufrufintervall ändern

Das RA-Sendeaufrufintervall ist die Zeit in Sekunden (s), Minuten (m) oder Stunden (h) zwischen den Abfragen der Arbeitsablaufswarteschlange durch den RA-Server. Die Elemente in dieser Warteschlange, deren Zuteilungszeit abgelaufen ist, werden für die Verarbeitung zugeteilt. So ändern Sie das Sendeaufrufintervall:

1. Melden Sie sich bei Ihrem Betriebssystem als Systemadministrator an.
2. Stoppen Sie das Tivoli PKI-System. Lesen Sie gegebenenfalls die Anweisungen unter „Serverkomponenten starten und stoppen” auf Seite 8 nach.
3. Laden Sie die Konfigurationsdatei ’jonahra.ini’ in einen Texteditor. Informationen zu den Dateipositionen unter AIX und Windows NT finden Sie in Tabelle 12 auf Seite 84.
4. Editieren Sie im Abschnitt **Transport** den Parameter **PollInterval**.
5. Ändern Sie den Wert des Sendeaufrufintervalls.
6. Speichern Sie die Datei.
7. Starten Sie das Tivoli PKI-System.

RA-Wiederholungsintervall ändern

Die Zeit zwischen den CA-Abfragen durch die RA in Sekunden (s), Minuten (m) oder Stunden (h), sofern der vom CA an die RA übermittelte Zeitpunkt für den Sendeaufruf vor der aktuellen Uhrzeit der RA liegt. So ändern Sie das RA-Wiederholungsintervall:

1. Melden Sie sich bei Ihrem Betriebssystem als Systemadministrator an.
2. Stoppen Sie das Tivoli PKI-System. Lesen Sie gegebenenfalls die Anweisungen unter „Serverkomponenten starten und stoppen" auf Seite 8 nach.
3. Laden Sie die Konfigurationsdatei 'jonahra.ini' in einen Texteditor. Informationen zu den Dateipositionen unter AIX und Windows NT finden Sie in Tabelle 12 auf Seite 84.
4. Editieren Sie im Abschnitt **Transport** den Parameter **RetryInterval**.
5. Ändern Sie den Wert des Wiederholungsintervalls.
6. Speichern Sie die Datei.
7. Starten Sie das Tivoli PKI-System.

RA-Serverprotokolle prüfen

Sie können die Protokolle des RA-Servers an den in Tabelle 5 angegebenen Positionen prüfen.

Tabelle 5. RA-Server-Protokolle

AIX-Standardpfad	Windows NT-Standardpfad	Beschreibung
/usr/lpp/iau/pkrf/Domains/YourDomain/logs/	c:\Program Files\IBM\Trust Authority\pkrf\Domains \YourDomain\logs\	Protokolldateien haben den Namen 'irgrasvr' und die Erweiterung '.log.zufällige_Nummer'.

Anmerkung: In der gelieferten Form protokolliert der RA-Server nicht die Betriebsaktivität. Der Abschnitt „Fehlerbehebung mit aktivierter Nachrichtenerstellung auf Debug-Stufe" auf Seite 135 enthält Anweisungen und Informationen zu empfohlenen Stufen, wenn Sie die RA-Server-Protokollierung auf Debug-Stufe aktivieren wollen.

RA-Serverstatus prüfen

Je nach Umgebung können Sie den Status des RA-Servers mit folgenden Prozeduren prüfen:

- Unter AIX:
  1. Melden Sie sich bei AIX als Root an.
  2. Prüfen Sie die Prozesstabelle, und suchen Sie nach folgender Zeichenfolge:
     ```
     irgrasvr
     ```
     Finden Sie diesen Prozess, fahren Sie mit Schritt 3 fort. Finden Sie diesen Prozess nicht, lesen Sie bitte im Abschnitt „Fehlerbehebung" auf Seite 135 nach.
  3. Wechseln Sie in das Verzeichnis 'bin'. Dieses Verzeichnis hat folgenden Standardpfad:
     ```
     /usr/lpp/iau/bin
     ```

4. Stellen Sie sicher, dass Port 29783 erfolgreich antwortet und geben Sie hierzu folgenden Befehl ein:

   ServerControl -i -c -k RA -n *Server* **-p 29783 -l "***Protokolldatei***"**

   Hierbei steht *Server* für den Namen des RA-Servers, der Port 29783 zugeordnet ist, und *Protokolldatei* für den Namen der Datei, in der die Ergebnisse des Befehls **ServerControl** aufgezeichnet werden sollen.

   Ist die Antwort des geprüften Ports erfolgreich, wird folgende Nachricht angezeigt:

   ```
   Es wurde
   festgestellt, dass der [RA]-Service auf dem Server am Anschluss 29783 ausgeführt wird.
   ```

   Hierbei steht *Server* für den Server, der Port 29783 zugeordnet ist.

- Unter Windows NT:
  1. Melden Sie sich bei Windows NT als Systemadministrator an.
  2. Starten Sie den Task-Manager durch Drücken der Tastenkombination **Strg**, **Alt** und **Entf**.
  3. Wählen Sie die Registerkarte **Prozesse** aus.
  4. Suchen Sie nach dem Prozess irgrasvr.exe.

     Finden Sie diesen Prozess, fahren Sie mit Schritt 5 fort. Finden Sie diesen Prozess nicht, lesen Sie bitte im Abschnitt „Fehlerbehebung” auf Seite 135 nach.
  5. Wechseln Sie an der MS DOS-Eingabeaufforderung in das Verzeichnis ’bin’. Dieses Verzeichnis hat folgenden Standardpfad:

     ```
     c:\Program Files\IBM\Trust Authority\bin
     ```
  6. Stellen Sie sicher, dass Port 29783 erfolgreich antwortet und geben Sie hierzu folgenden Befehl ein:

     ServerControl -i -c -k CA -n *Server* **-p 29783 -l "***Protokolldatei***"**

     Hierbei steht *Server* für den Namen des RA-Servers, der Port 29783 zugeordnet ist, und *Protokolldatei* für den Namen der Datei, in der die Ergebnisse des Befehls **ServerControl** aufgezeichnet werden sollen.

     Ist die Antwort des geprüften Ports erfolgreich, wird folgende Nachricht angezeigt:

     ```
     Es wurde
     festgestellt, dass der [RA]-Service auf dem Server am Anschluss 29783 ausgeführt wird.
     ```

     Hierbei steht *Server* für den Server, der Port 29783 zugeordnet ist.

RA-Einstellungen für die Kommunikation mit dem Directory ändern

Der RA-Server kommuniziert mit dem IBM Directory-Server, um den Registrierungsprozess zu verwalten. In der Konfigurationsdatei des RA-Servers können folgende Werte geändert werden, um die Kommunikation zwischen RA und Directory zu beeinflussen:

- Host-Name und Port des Directory-Servers
- Sendeintervall

RA-Einstellungen für Host-Namen und Port des Directory-Servers ändern

Für eine effiziente Kommunikation mit dem Directory benötigt die RA den korrekten Host-Namen und den korrekten Port, an dem das Directory empfangsbereit ist. So ändern Sie den Host-Namen und den Port, der von der RA für die Kommunikation mit dem Directory benötigt wird:

1. Melden Sie sich bei Ihrem Betriebssystem als Systemadministrator an.
2. Stoppen Sie das Tivoli PKI-System. Lesen Sie gegebenenfalls die Anweisungen unter „Serverkomponenten starten und stoppen" auf Seite 8 nach.
3. Laden Sie die Konfigurationsdatei 'jonahra.ini' in einen Texteditor. Informationen zu den Dateipositionen unter AIX und Windows NT finden Sie in Tabelle 12 auf Seite 84.
4. Editieren Sie im Abschnitt **LDAP** den Parameter **Server1**.
5. Ändern Sie die Werte für den Host-Namen und die Port-Nummer.
6. Speichern Sie die Datei.
7. Starten Sie das Tivoli PKI-System.

RA-Einstellungen für das Sendeintervall des Directory-Servers ändern

Das Sendeintervall ist der Zeitraum, in dem die RA nicht prüft, ob Informationen zum Senden an das Directory vorliegen. Zu diesen Informationen zählen beispielsweise neue Benutzerzertifikate oder neue CRLs.

So ändern Sie das Sendeintervall der RA:

1. Melden Sie sich bei Ihrem Betriebssystem als Systemadministrator an.
2. Stoppen Sie das Tivoli PKI-System. Lesen Sie gegebenenfalls die Anweisungen unter „Serverkomponenten starten und stoppen" auf Seite 8 nach.
3. Laden Sie die Konfigurationsdatei 'jonahra.ini' in einen Texteditor. Informationen zu den Dateipositionen unter AIX und Windows NT finden Sie in Tabelle 12 auf Seite 84.
4. Editieren Sie im Abschnitt **LDAP** den Parameter **PostInterval**.
5. Ändern Sie den Wert des Parameters 'PostInterval'.
6. Speichern Sie die Datei.
7. Starten Sie das Tivoli PKI-System.

Übergabe der Trust-Kette aktivieren bzw. inaktivieren

Bei der Installation des CA-Servers ist die Übergabe der Trust-Kette standardmäßig inaktiviert. Die Übergabe der Trust-Kette können Sie aktivieren bzw. inaktivieren, indem Sie den Wert eines Parameters in der Datei 'jonahra.ini' ändern.

So aktivieren bzw. inaktivieren Sie die Übergabe der Trust-Kette:

1. Melden Sie sich bei Ihrem Betriebssystem als Systemadministrator an.
2. Stoppen Sie das Tivoli PKI-System. Lesen Sie gegebenenfalls die Anweisungen unter „Serverkomponenten starten und stoppen" auf Seite 8 nach.
3. Laden Sie die Konfigurationsdatei 'jonahra.ini' in einen Texteditor. Informationen zu den Dateipositionen unter AIX und Windows NT finden Sie in Tabelle 12 auf Seite 84.
4. Editieren Sie im Abschnitt **General** den Parameter **TrustChainDelivery**.

5. Ändern Sie den Wert in **1**, um die Übergabe der Trust-Kette zu aktivieren. Zur Inaktivierung geben Sie den Wert **0** an.
6. Speichern Sie die Datei.
7. Starten Sie das Tivoli PKI-System.

Mehrere RAs installieren

Tivoli PKI unterstützt die Installation von mehreren RA-Servern (MRA) unter einem CA. Auf diese Weise können Sie verschiedene RA-Server für unterschiedliche Zwecke definieren. Eine Situation, in der dies erforderlich sein könnte, wäre beispielsweise eine Muttergesellschaft, die für ihre einzelnen Tochtergesellschaften unterschiedliche Zertifikattypen ausstellen muss. Dies wird durch die Einrichtung mehrerer RAs möglich. Jede RA verwendet denselben CA, kann jedoch Zertifikate anhand unterschiedlicher Regeln ausstellen. MRAs müssen auf einem anderen Server als der ursprüngliche CA und die ursprüngliche RA installiert werden. Die Installation von mehreren RAs ähnelt in vielen Punkten der Installation der ersten RA. Um zusätzliche RAs zu installieren, lesen und befolgen Sie die Anweisungen in den folgenden Abschnitten.

Anmerkung: Sie können eine MRA erst nach der Erstinstallation von CA und RA installieren.

Tivoli PKI auf MRA-System installieren

Tivoli PKI kann so installiert werden, wie Sie möchten. Alle Konfigurationsoptionen sind zulässig. Befolgen Sie hierzu die Anweisungen im Handbuch *Tivoli PKI Einführung*. Sobald Sie die Erstinstallation vorgenommen haben, kehren Sie jedoch zu den vorliegenden Anweisungen zurück. Bitte führen Sie jetzt noch keine der Dienstprogramme aus, die nach der Installation oder nach der Konfiguration verwendet werden können.

Datei 'mraConfig.dat' für neue MRA erstellen

Für jede Installation einer MRA wird eine Datei 'mraConfig.dat' benötigt. Sie können für jede installierte MRA eine neue Datendatei erstellen oder auch jedes Mal dieselbe Datei verwenden. Die Datendatei enthält die Position, das Zertifikat und den elektronischen Fingerabdruck des CA. Mit dem Dienstprogramm Create New RA können Sie sie auf dem CA erstellen. Weitere Informationen zum Dienstprogramm Create New RA finden Sie unter „Befehlszeilendienstprogramme" auf Seite 112. Das Dienstprogramm Create New RA erstellt die Datendatei basierend auf der Datei 'mraTemplate.ini'. Name und Zielposition der Ausgabedatei können mit dem Befehlszeilenparameter **-f** angegeben werden. Andernfalls wird die Datendatei mit 'mraConfig.dat' benannt und im aktuellen Arbeitsverzeichnis gespeichert.

Datei 'mraConfig.dat' an MRA-Server übertragen

Sobald die Datei 'mraConfig.dat' erstellt wurde, müssen Sie sie über eine gesicherte Methode im Offlinemodus an das System übertragen, auf dem Sie die MRA definieren wollen. Der Inhalt der Datei sollte während der Übertragung vor Manipulationen geschützt sein. Da die Datendatei jedoch das Zertifikat des CA enthält, sollte der CA nicht zum Unterzeichnen der Datei verwendet werden. Sie müssen dafür sorgen, dass die Integrität der Datei während der Übertragung an die MRA-Maschine gewährleistet ist. Speichern Sie die Datei 'mraConfig.dat' im Verzeichnis '/usr/lpp/iau/bin'.

CfgPostInstall auf MRA-Server ausführen

Nachdem Sie die Datei 'mraConfig.dat' an das System übertragen haben, auf dem Sie eine neue MRA definieren wollen, führen Sie den Befehl 'CfgPostInstall' mit dem Parameter **-m**, gefolgt vom Namen der Datei 'mraConfig.dat', aus. Weitere Informationen zum Befehl 'CfgPostInstall' finden Sie unter „Befehlszeilendienstprogramme" auf Seite 112. Der Befehl 'CfgPostInstall' nimmt anhand der Informationen in der Datei 'mraConfig.dat' eine Anpassung der Anzeigen im Setup Wizard vor und ermöglicht die Erstellung einer MRA.

Setup Wizard auf MRA-Server ausführen

Als Nächstes muss der Setup Wizard auf der MRA-Maschine ausgeführt werden. Hierzu starten Sie den Browser, und geben Sie die Adresse des MRA-Servers ein (z. B.: https://webserver.tivoli.com/). Im Browser wird dieselbe Seite angezeigt, die auch bei der Konfiguration des ersten CA bzw. der ersten RA verwendet wird. Befolgen Sie die Anweisungen auf der Seite, um die Datei 'swingall.jar' herunterzuladen, und klicken Sie anschließend auf den Link zum Setup Wizard. Der Setup Wizard stellt automatisch fest, dass der erste Abschnitt einer MRA-Installation vorliegt, und ermöglicht Ihnen die Anpassung und Bestätigung der Parameter für die MRA. Sobald die Verarbeitung des Setup Wizard beendet ist, erstellt er eine Vorabregistrierungsdatei für die MRA. Der Setup Wizard zeigt den Pfad an, in dem die Vorabregistrierungsdatei gespeichert wurde.

Vorabregistrierungsdatei an CA-Server übertragen

Die Vorabregistrierungsdatei enthält Informationen zur MRA, die Sie definieren. Diese Informationen werden durch den CA verarbeitet und dienen zur Berechtigung der MRA. Sie müssen die Vorabregistrierungsdatei mit einer gesicherten Methode im Offlinemodus an den CA-Server übertragen. Sie müssen dafür sorgen, dass die Integrität der Datei während der Übertragung an den CA geschützt bleibt. Speichern Sie die Datei auf dem CA-Server im Verzeichnis '/usr/lpp/iau/bin'.

MRA-Registrierung auf CA-Server berechtigen

Nachdem Sie die Vorabregistrierungsdatei an den CA-Server übertragen haben, muss der CA-Server die MRA genehmigen. Dies erfolgt über den Befehl *authRAEnrollment*. Für diesen Befehl muss der Parameter **-f**, gefolgt vom Namen der Vorabregistrierungsdatei, verwendet werden. Weitere Informationen zum Befehl 'authRAEnrollment' finden Sie unter „Befehlszeilendienstprogramme" auf Seite 112. Dies berechtigt das Zertifikat von der MRA und bereitet den CA so vor, dass Anforderungen von der MRA akzeptiert werden können.

Setup Wizard erneut auf MRA-Server ausführen

Der letzte Schritt ist die erneute Ausführung des Setup Wizard auf dem MRA-Server. Wenn Ihr Browser noch mit der Konfigurationsseite geöffnet ist, laden Sie den Browser erneut, indem Sie die Umschalttaste gedrückt halten und auf die Option für das erneute Laden klicken. Hierdurch wird die Seite erneut geladen, und zwar nicht aus dem Cache, sondern aus dem Server. Sie können auch den Browser schließen und erneut mit der Konfigurationsseite öffnen. Klicken Sie wieder auf den Link für den Setup Wizard. Der Setup Wizard ruft automatisch die letzte Anzeige auf. Klicken Sie auf **Fertig stellen**, und warten Sie, bis die Konfiguration abgeschlossen ist. Nach Abschluss der Konfiguration ist die neue MRA definiert und einsatzbereit.

Prüfsubsystem verwalten

Zur Verwaltung des Prüfsubsystems müssen Sie die Funktion des Prüfadministrators übernehmen. Für einige dieser Verwaltungs-Tasks ist ein Kennwort erforderlich. Informationen zum Ändern des Kennworts für den Prüfadministrator finden Sie im Abschnitt „Tivoli PKI-Kennwörter ändern” auf Seite 5.

Der Prüf-Server ist ein Tivoli PKI-Prozess, der Prüfereignisse von Tivoli PKI-Komponenten empfängt und diese in einem Prüfprotokoll aufzeichnet. Er befindet sich zusammen mit seinem DB2-Datenbankexemplar auf einer lokalen oder fernen Maschine. Der Prüf-Server muss sich auf der gleichen Maschine befinden, wie der CA-Server.

Die folgenden Tasks zur Verwaltung des Prüfsubsystems werden beschrieben:

- Verwendung der beiden Tivoli PKI-Datenbanksichten zum Anzeigen von Protokolleinträgen in der Prüfdatenbank
- Verwendung der DB2 UDB-Tools zur Suche nach Protokolleinträgen oder zum Generieren von Prüfberichten
- Vornahme der folgenden Änderungen an der Konfigurationsdatei ’AuditClient.ini’ mit einem Texteditor:
  - Ändern des Ports für den Prüfserver
  - Ändern der Sendeart für Ereignisse vom Prüf-Client
- Vornahme der folgenden Änderungen an der Konfigurationsdatei ’AuditServer.ini’ mit einem Texteditor:
  - Ändern des Listener-Ports für den Prüfserver
  - Ändern der Anzahl von Wiederholungen, mit denen der Prüf-Client versucht, eine Verbindung zum Prüfserver herzustellen
  - Ändern der Zeit zwischen Verbindungsversuchen
  - Ändern der Protokolleinstellungen für Ereignis-, Prüf-, Trace- und Fehlerprotokolle
- Verwendung des Dienstprogramms ’Audit Archive and Sign’ zur Archivierung und Unterzeichnung von Prüfprotokolldateien
- Verwendung des Dienstprogramms ’Audit Integrity Check’ zur Prüfung der Integrität von Datenbank- und Archivierungsdateien auf dem Prüfserver
- Prüfen des Status des Prüfservers
- Prüfen der Prüfserverprotokolle

Protokolleinträge anzeigen

Sie können sich die Protokolleinträge in der DB2-Prüfdatenbank mit Hilfe von zwei Tivoli PKI-Sichten anzeigen lassen. Diese Datenbanksichten zeigen alle derzeit in der Datenbank gespeicherten Protokolleinträge an. Die Protokolleinträge werden in der Datenbanktabelle 'audit_log' gespeichert. Bei den meisten Spalten dieser Tabelle handelt es sich um kurze Integer-Codes, die auf andere Tabellen verweisen. Diese anderen Tabellen enthalten die vollständige Beschreibung oder die Namen der Felder des Protokolleintrags. (Diese Felder entsprechen in der Datenbank den Spalten einer Tabelle.) Informationen zu Feldnamen und Beschreibungen aller Tabellen im Prüfdatenbankschema finden Sie im Abschnitt „Prüfung von Datenbankdaten" auf Seite 129.

Folgende Sichten sind verfügbar:

- viewar

  Dies ist die grundlegende Sicht, die den Zugriff auf alle Textbeschreibungen (ungekürzt) ermöglicht.

- viewar_t

  Diese Sicht entspricht der Sicht viewar, die Textspalten werden jedoch nach 40 Zeichen abgeschnitten.

  Anmerkung: Wenn Sie die Datenbank 'viewar_t' unter Windows NT über die Schnittstelle der DB2-Steuerzentrale abfragen, wird aufgrund des Abschneidens beim Auswählen der Option für den Beispielinhalt eine leere Ausgabe angezeigt. Die in diesem Abschnitt dokumentierte Prozedur bietet eine Möglichkeit, dieses Problem zu umgehen.

Die Sichten verfügen über die in Tabelle 6 angegebenen Spaltennamen.

Tabelle 6. Spaltenbeschreibungen der Sichten für die Tivoli PKI-Prüfdatenbank

Spaltenname	Beschreibung	Datentyp
serial_num	Die Seriennummer des Protokolleintrags	integer
sourcetime	Die Zeitmarke, die angibt, wann das Prüfereignis durch den Client erstellt wurde.	timestamp
createtime	Die Zeitmarke, die angibt, wann der Protokolleintrag erstellt wurde.	timestamp
Ereignis	Der Name des Ereignisses	varchar
source	Der Prüf-Client, der das Prüfereignis generiert hat.	varchar
component	Die Komponentenart des Prüf-Clients, der das Prüfereignis generiert hat.	varchar
auth_entity	Die Entität, die das Prüfereignis berechtigt hat.	varchar
auth_role	Der Aufgabenbereich der Entität, die das Prüfereignis berechtigt hat.	varchar

Tabelle 6. Spaltenbeschreibungen der Sichten für die Tivoli PKI-Prüfdatenbank (Forts.)

Spaltenname	Beschreibung	Datentyp
affected_entity	Die Kennung der Entität, die von einem Prüfereignis betroffen ist.	varchar
affected_entity_type	Die Art der betroffenen Entität.	varchar
storage_media	Das dem Prüfereignis zugeordnete Speichermedium.	varchar
extra_info	Dem Prüfereignis zugeordnete Zusatzinformationen.	varchar

So können Sie sich die Sätze in der Tivoli PKI-Prüfdatenbank anzeigen lassen:

1. Melden Sie sich bei Tivoli PKI als der Benutzer an, der Tivoli PKI installiert hat.
2. Starten Sie eine interaktive DB2-Befehlszeilensitzung.

   Anmerkung: Wenn Sie Windows NT ausführen, hat eine während des Installationsabschlusses definierte Codepage-Variable möglicherweise dazu geführt, dass in den CHAR- und VARCHAR-Spalten im DB2-Befehlsfenster falsche Zeichen angezeigt werden. Um dies zu beheben, geben Sie vor der Eingabe von DB2-SQL-Anweisungen die folgenden Befehle ein:

   ```
   set DB2CODEPAGE=
   db2 terminate
   ```

   Starten Sie die DB2-Sitzung anschließend erneut.
3. Geben Sie an der DB2-Befehlszeile den folgenden Befehl ein, um eine Verbindung zur Prüfdatenbank herzustellen:

   ```
   connect to
   Name_Ihrer_Prüfdatenbank
   ```

   Geben Sie beispielsweise für die Datenbank namens ’adtdb’ folgenden Befehl ein:

   ```
   connect to adtdb
   ```
4. Fragen Sie die Datenbank wie nachfolgend beschrieben mit Hilfe einer Tivoli PKI-Sicht ab.

   - Geben Sie für eine Abfrage mit der Sicht viewvar folgenden Befehl ein:

     ```
     "select * from viewvar"
     ```
   - Geben Sie für eine Abfrage mit der Sicht viewvar_t folgenden Befehl ein:

     ```
     "select * from viewvar_t"
     ```

     Das System zeigt für alle Einträge der Prüfdatenbank die in Tabelle 6 auf Seite 47 beschriebenen Spalten an.

5. Verwenden Sie zum Filtern der Sicht für die Protokolleinträge die SQL-Klausel **where**. Geben Sie beispielsweise folgenden Befehl ein, um Einträge auf einen bestimmten Datumsbereich zu beschränken:

```
"select * from viewvar where sourcetime between '1999-07-01-08.00.00' and
 '1999-07-02-08.00.00'"
```

   Details zur SQL-Anweisung **select** finden Sie im Handbuch *IBM DB2 Universal Database SQL Reference*. Ausführliche Informationen zum Befehl **db2** enthält das Handbuch *IBM DB2 Universal Database Command Reference*.

Protokolleinträge suchen

Anweisungen zum Suchen nach Protokolleinträgen finden Sie im Handbuch *IBM DB2 Universal Database SQL Reference*.

Prüfserver-Port auf dem Prüf-Client ändern

Der Prüfserver-Port ist der Port, an dem der Prüfserver für neue Verbindungen vom Prüf-Client empfangsbereit ist. Für eine effiziente Kommunikation zwischen Prüf-Client und Prüf-Server muss der Prüf-Client über den korrekten Port des Prüf-Servers verfügen. So ändern Sie um die Werte für den Port des Prüfservers in der Konfigurationsdatei des Prüf-Clients:

1. Melden Sie sich bei Ihrem Betriebssystem als Systemadministrator an.
2. Stoppen Sie das Tivoli PKI-System. Lesen Sie gegebenenfalls die Anweisungen unter „Serverkomponenten starten und stoppen” auf Seite 8 nach.
3. Laden Sie die Konfigurationsdatei ’AuditClient.ini’ in einen Texteditor. Informationen zu den Dateipositionen unter AIX und Windows NT finden Sie in Tabelle 12 auf Seite 84.
4. Editieren Sie im Abschnitt **Connection** den Parameter **Port**.
5. Ändern Sie den Wert für den Port des Prüfservers.
6. Speichern Sie die Datei.
7. Starten Sie das Tivoli PKI-System.
8. Stellen Sie sicher, dass der geänderte Port-Wert dem Wert des Parameters ’acceptor.arg’ in der Datei AuditServer.ini’ entspricht. Diese Datei befindet sich auf dem Prüf-Server.

Sendeart für Ereignisse vom Prüf-Client ändern

Der Prüf-Client sendet Prüfereignisse an den Prüf-Server. Sie können das Senden bestimmter Ereignisse an den Prüf-Server unterbinden, indem Sie in der Datei ’AuditClient.ini’ eine Prüfmaske definieren. Einige Ereignisse müssen jedoch immer gesendet werden.

Informationen zu verbindlichen und optionalen Prüfereignissen finden Sie im Abschnitt „Prüfereignisse” auf Seite 126. Darüber hinaus können Sie auch die Anzahl der Wiederholungsversuche nach dem ersten Sendeversuch des Prüf-Clients an den Prüfserver definieren. Sie können auch die Zeit in Millisekunden angeben, die zwischen den Wiederholungsversuchen für das Herstellen einer Verbindung zum Server gewartet werden soll.

Prüfmaske definieren

So definieren Sie eine Prüfmaske:

1. Melden Sie sich bei Ihrem Betriebssystem als Systemadministrator an.
2. Stoppen Sie das Tivoli PKI-System. Lesen Sie gegebenenfalls die Anweisungen unter „Serverkomponenten starten und stoppen” auf Seite 8 nach.

3. Laden Sie die Konfigurationsdatei 'AuditClient.ini' in einen Texteditor. Informationen zu den Dateipositionen unter AIX und Windows NT finden Sie in Tabelle 12 auf Seite 84.
4. Editieren Sie im Abschnitt **CA** den Parameter **ExcludedEvents**.
5. Fügen Sie die Namen der vom CA generierten Prüfereignisse hinzu, die vom Prüf-Client zurückgehalten werden sollen. Die Namen der Prüfereignisse müssen durch Kommas getrennt werden. Geben Sie nur optionale Ereignisse an.
6. Editieren Sie im Abschnitt **RA** den Parameter **ExcludedEvents**.
7. Fügen Sie die Namen der vom RA generierten Prüfereignisse hinzu, die vom Prüf-Client zurückgehalten werden sollen. Die Namen der Prüfereignisse müssen durch Kommas getrennt werden. Geben Sie nur optionale Ereignisse an. Informationen zu den Namen von Prüfereignissen finden Sie im Abschnitt „Prüfereignisse" auf Seite 126.
8. Speichern Sie die Datei.
9. Starten Sie das Tivoli PKI-System.

Anzahl der Wiederholungen für das Senden von Ereignissen ändern

So ändern Sie die Anzahl von Wiederholungsversuchen nach dem ersten Sendeversuch des Prüf-Clients:

1. Melden Sie sich bei Ihrem Betriebssystem als Systemadministrator an.
2. Stoppen Sie das Tivoli PKI-System. Lesen Sie gegebenenfalls die Anweisungen unter „Serverkomponenten starten und stoppen" auf Seite 8 nach.
3. Laden Sie die Konfigurationsdatei 'AuditClient.ini' in einen Texteditor. Informationen zu den Dateipositionen unter AIX und Windows NT finden Sie in Tabelle 12 auf Seite 84.
4. Editieren Sie im Abschnitt **Connection** den Parameter **Retries**.
5. Ändern Sie den Wert des Parameters **Retries**.
6. Speichern Sie die Datei.
7. Starten Sie das Tivoli PKI-System.

Intervall zwischen Wiederholungsversuchen ändern

So ändern Sie das Intervall zwischen Wiederholungsversuchen:

1. Melden Sie sich bei Ihrem Betriebssystem als Systemadministrator an.
2. Stoppen Sie das Tivoli PKI-System. Lesen Sie gegebenenfalls die Anweisungen unter „Serverkomponenten starten und stoppen" auf Seite 8 nach.
3. Laden Sie die Konfigurationsdatei 'AuditClient.ini' in einen Texteditor. Informationen zu den Dateipositionen unter AIX und Windows NT finden Sie in Tabelle 12 auf Seite 84.
4. Editieren Sie im Abschnitt **Connection** den Parameter **Timer**.
5. Ändern Sie den Wert des Parameters 'Timer'.
6. Speichern Sie die Datei.
7. Starten Sie das Tivoli PKI-System.

Listener-Port für den Prüfserver ändern

Der Prüfserver-Port ist der Port, an dem der Prüfserver für neue Verbindungen vom Prüf-Client empfangsbereit ist. So können Sie die Port-Werte für den Prüfserver in der Konfigurationsdatei des Prüfservers ändern:

1. Melden Sie sich bei Ihrem Betriebssystem als Systemadministrator an.
2. Stoppen Sie das Tivoli PKI-System. Lesen Sie gegebenenfalls die Anweisungen unter „Serverkomponenten starten und stoppen" auf Seite 8 nach.
3. Laden Sie die Konfigurationsdatei 'AuditServer.ini' in einen Texteditor. Informationen zu den Dateipositionen unter AIX und Windows NT finden Sie in Tabelle 12 auf Seite 84.
4. Editieren Sie im Abschnitt **Server Port** den Parameter **acceptor.arg**.
5. Ändern Sie den Wert der Port-Nummer.
6. Speichern Sie die Datei.
7. Starten Sie das Tivoli PKI-System.
8. Stellen Sie sicher, dass der geänderte Server-Port an alle lokalen und fernen Dateien vom Typ 'AuditClient.ini' weitergegeben wird. Nähere Informationen hierzu finden Sie im Abschnitt „Prüfserver-Port auf dem Prüf-Client ändern" auf Seite 49.

Anzahl der Bindungsversuche zwischen Prüfserver und Prüf-Client ändern

So ändern Sie die Anzahl der Bindungsversuche des Prüf-Clients:

1. Melden Sie sich bei Ihrem Betriebssystem als Systemadministrator an.
2. Stoppen Sie das Tivoli PKI-System. Lesen Sie gegebenenfalls die Anweisungen unter „Serverkomponenten starten und stoppen" auf Seite 8 nach.
3. Laden Sie die Konfigurationsdatei 'AuditServer.ini' in einen Texteditor. Informationen zu den Dateipositionen unter AIX und Windows NT finden Sie in Tabelle 12 auf Seite 84.
4. Editieren Sie im Abschnitt **Server Port** den Parameter **acceptor.init.retries**.
5. Ändern Sie den Wert für die Bindungsversuche. Die Standardeinstellung ist **3**.
6. Speichern Sie die Datei.
7. Starten Sie das Tivoli PKI-System.

Intervall zwischen Bindungsversuchen ändern

So ändern Sie das Intervall zwischen den Bindungsversuchen des Prüf-Clients:

1. Melden Sie sich bei Ihrem Betriebssystem als Systemadministrator an.
2. Stoppen Sie das Tivoli PKI-System. Lesen Sie gegebenenfalls die Anweisungen unter „Serverkomponenten starten und stoppen" auf Seite 8 nach.
3. Laden Sie die Konfigurationsdatei 'AuditServer.ini' in einen Texteditor. Informationen zu den Dateipositionen unter AIX und Windows NT finden Sie in Tabelle 12 auf Seite 84.
4. Editieren Sie im Abschnitt **Server Port** den Parameter **acceptor.init.delay**.
5. Ändern Sie den in Sekunden angegebenen Wert für die Zeit zwischen zwei Bindungsversuchen. Die Standardeinstellung ist **3** (das Programm geht von Sekunden aus).
6. Speichern Sie die Datei.
7. Starten Sie das Tivoli PKI-System.

Protokolleinstellungen ändern

Sie können die Einstellungen in der Datei 'AuditServer.ini' für folgende Protokolltypen ändern:

- Ereignisprotokoll - Zur Aufzeichnung von Prüfereignissen
- Prüfprotokoll - Zur Speicherung integritätsgeschützter Prüfereignisse in der Datenbank
- Trace-Protokoll - Zur Aufzeichnung von Programmaktivitäten
- Fehlerprotokoll - Zur Aufzeichnung von Fehlernachrichten

Aufzeichnungsart für Prüfereignisse ändern

Das Ereignisprotokoll ist eine Datei zur Aufzeichnung von Ereignissen. Sie können folgende Konfigurationsparameter ändern:

- Den Dateinamen und den Pfad des Ereignisprotokolls
- Die Markierung, die angibt, ob Daten an das bereits vorhandene Ereignisprotokoll angefügt werden oder ob diese überschrieben wird.

So können Sie die Einstellungen für das Aufzeichnen von Ereignissen ändern:

1. Melden Sie sich bei Ihrem Betriebssystem als Systemadministrator an.
2. Stoppen Sie das Tivoli PKI-System. Lesen Sie gegebenenfalls die Anweisungen unter „Serverkomponenten starten und stoppen" auf Seite 8 nach.
3. Laden Sie die Konfigurationsdatei 'AuditServer.ini' in einen Texteditor. Informationen zu den Dateipositionen unter AIX und Windows NT finden Sie in Tabelle 12 auf Seite 84.
4. Editieren Sie den Abschnitt **Event Log**. Weitere Schritte:
   - So ändern Sie den Pfad oder den Dateinamen des Ereignisprotokolls:
     a. Editieren Sie den Parameter **event.log.filename**.
     b. Ändern Sie den Wert für den Pfad oder den Dateinamen.
   - So ändern Sie die Markierung, die angibt, ob das Daten an das bereits vorhandende Ereignisprotokoll angefügt werden oder ob dieses überschrieben wird:
     a. Editieren Sie den Parameter **event.log.append**.
     b. Ändern Sie den Wert des Parameters. Geben Sie **true** zum Anfügen bzw. **false** zum Überschreiben an.
5. Speichern Sie die Datei.
6. Starten Sie das Tivoli PKI-System.

Protokollierung von Prüfereignissen in der Datenbank ändern

Das Prüfprotokoll besteht aus einer Reihe von integritätsgeschützten Datenbanktabellen, die zur Speicherung von Prüfereignissen verwendet werden. Das Prüfprotokoll enthält pro Prüfereignis einen Protokolleintrag. Sie können folgende Konfigurationsparameter ändern:

- Die Anzahl der zulässigen Versuche zur Herstellung einer Verbindung mit der Prüfprotokolldatenbank
- Die Anzahl der zulässigen Versuche zur Aktualisierung der Prüfprotokolldatenbank

- Den zulässigen Zeitlimitüberschreitungswert (in Sekunden) zur Aktualisierung des Prüfprotokolls

So können Sie die Einstellungen für das Protokollieren von Prüfereignissen ändern:

1. Melden Sie sich bei Ihrem Betriebssystem als Systemadministrator an.
2. Stoppen Sie das Tivoli PKI-System. Lesen Sie gegebenenfalls die Anweisungen unter „Serverkomponenten starten und stoppen" auf Seite 8 nach.
3. Laden Sie die Konfigurationsdatei 'AuditServer.ini' in einen Texteditor. Informationen zu den Dateipositionen unter AIX und Windows NT finden Sie in Tabelle 12 auf Seite 84.
4. Editieren Sie den Abschnitt **Audit**. Weitere Schritte:
   - Ändern Sie die Anzahl der zulässigen Versuche zur Herstellung einer Verbindung mit der Prüfprotokolldatenbank wie folgt:
     a. Editieren Sie den Parameter **audit.log.connect.retries**.
     b. Ändern Sie den Wert des Parameters. Der Wert muss eine ganze Zahl sein.
   - Ändenr Sie die Anzahl der zulässigen Versuche zur Aktualisierung des Prüfprotokolls wie folgt:
     a. Wählen Sie den Parameter **audit.log.update.retries** aus.
     b. Ändern Sie im angezeigten Editierfeld den Wert des Parameters. Sie müssen einen Integer-Wert eingeben.
   - Ändern Sie den zulässigen Zeitlimitüberschreitungswert zur Aktualisierung des Prüfprotokolls wie folgt:
     a. Wählen Sie den Parameter **audit.log.timeout** aus.
     b. Ändern Sie im angezeigten Editierfeld den Wert des Parameters. Sie müssen ein Zeitintervall eingeben.
5. Speichern Sie die Datei und beenden Sie das Programm.
6. Starten Sie das Tivoli PKI-System.

Einstellungen für Trace-Protokoll ändern

Das Trace-Protokoll enthält Aufzeichnungen zur Ausführung eines Computerprogramms. Es gibt die Reihenfolge der Ausführung von Anweisungen wider. Dieses Protokoll wird primär zur Fehlerbehebung verwendet. Sie können folgende Konfigurationsparameter ändern:

- Aktivieren/Inaktivieren der Trace-Funktion
- Die Trace-Stufe
- Dateiname und Pfad des Trace-Protokolls
- Die Markierung, die angibt, ob Daten an die bereits vorhandene Trace-Datei angefügt werden oder ob diese überschrieben wird.

So ändern Sie die Einstellungen für das Trace-Protokoll ändern:

1. Melden Sie sich bei Ihrem Betriebssystem als Systemadministrator an.
2. Stoppen Sie das Tivoli PKI-System. Lesen Sie gegebenenfalls die Anweisungen unter „Serverkomponenten starten und stoppen" auf Seite 8 nach.

3. Laden Sie die Konfigurationsdatei 'AuditServer.ini' in einen Texteditor. Informationen zu den Dateipositionen unter AIX und Windows NT finden Sie in Tabelle 12 auf Seite 84.
4. Editieren Sie den Abschnitt **Trace**. Weitere Schritte:
   - Aktivieren bzw. inaktivieren Sie die Trace-Funktion wie folgt:
     a. Editieren Sie den Parameter **trace.enable**.
     b. Ändern Sie den Wert des Parameters. Geben Sie **true** zum Aktivieren bzw. **false** zum Inaktivieren an.
   - Ändern Sie die Trace-Stufe wie folgt:
     a. Editieren Sie den Parameter **trace.level.name**.
     b. Ändern Sie den Wert des Parameters. Sie müssen eine Zeichenfolge eingeben. Eine Liste der Trace-Stufen finden Sie im Abschnitt „Trace-Stufen" auf Seite 105.
   - Ändern Sie folgendermaßen Dateiname und Pfad des Trace-Protokolls:
     a. Editieren Sie den Parameter **trace.log.filename**.
     b. Ändern Sie den Wert des Parameters. Sie müssen eine Zeichenfolge eingeben.
   - So können Sie die Markierung ändern, die angibt, ob Daten an die bereits vorhandene Trace-Datei angefügt werden oder ob diese überschrieben wird:
     a. Editieren Sie den Parameter **trace.log.append**.
     b. Ändern Sie den Wert des Parameters. Geben Sie **true** zum Anfügen bzw. **false** zum Überschreiben an.
5. Speichern Sie die Datei.
6. Starten Sie das Tivoli PKI-System.

Dateinamen und Pfad des Fehlerprotokolls ändern

Das Fehlerprotokoll enthält Fehlernachrichten des Prüfsubsystems. So können Sie den Dateinamen und den Pfad des Fehlerprotokolls ändern:

1. Melden Sie sich bei Ihrem Betriebssystem als Systemadministrator an.
2. Stoppen Sie das Tivoli PKI-System. Lesen Sie gegebenenfalls die Anweisungen unter „Serverkomponenten starten und stoppen" auf Seite 8 nach.
3. Laden Sie die Konfigurationsdatei 'AuditClient.ini' in einen Texteditor. Informationen zu den Dateipositionen unter AIX und Windows NT finden Sie in Tabelle 12 auf Seite 84.
4. Editieren Sie im Abschnitt **Error** den Parameter **error.log.filename**.
5. Ändern Sie den Wert des Parameters 'error.log.filename'.
6. Speichern Sie die Datei.
7. Starten Sie das Tivoli PKI-System.

Prüfberichte generieren

Anweisungen zum Generieren von Prüfberichten finden Sie im Handbuch *IBM DB2 Universal Database SQL Reference*.

Prüfprotokolldateien archivieren und unterzeichnen

Mit dem Tivoli PKI-Tool Audit Archive and Sign können Sie Prüfprotokolldateien archivieren und unterzeichnen. Dieses Tool archiviert die Tabellen der Datenbank des Prüf-Servers, die Prüfsätze enthalten. Die Tabellen werden mit Hilfe des DB2-Exportdienstprogramms in einer Datei archiviert. Anschließend wird die Datei unterzeichnet. Alle Prüfsätze werden nach erfolgreicher Archivierung aus der Datenbank entfernt, wenn die Option -n nicht angegeben wird.

Anmerkung: Das Tivoli PKI-System muss vor der Ausführung dieses Dienstprogramms nicht heruntergefahren werden.

Angenommen, Sie verwenden den standardmäßigen Tivoli PKI-Installationspfad. Sie möchten die aktuellen Prüfsätze der Datenbank des Prüf-Servers in der Datei 'meine.datei' archivieren und diese Datei unterzeichnen. Die Prüfsätze sollen jedoch nicht aus der Datenbank entfernt werden. Gehen Sie wie folgt vor:

1. Melden Sie sich bei Tivoli PKI als Konfigurationsbenutzer an der Maschine an, auf der die Tivoli PKI-CA- und Prüf-Server-Komponente installiert ist.

   Der empfohlene Benutzername, der gleichzeitig auch der Standardbenutzername ist, lautet **cfguser**. Wenn Tivoli PKI unter Windows NT installiert ist, wurde vom jeweiligen Unternehmen möglicherweise ein anderer Benutzername verwendet.

2. Geben Sie in der Befehlszeile Ihrer Umgebung folgenden Befehl ein:

   - Unter AIX:

     ```
     AuditArchiveAndSign -c /usr/lpp/iau/etc/TrustAuthority/AuditServer.ini -n
          /usr/lpp/iau/arc/meine.datei
     ```

   - Unter Windows NT:

     ```
     AuditArchiveAndSign -c "d:\Program Files\IBM\Trust Authority\etc\TrustAuthority\
        AuditServer.ini" -n "d:\Program Files\IBM\Trust
     Authority\arc\meine.datei"
     ```

3. Wenn das System Sie zur Eingabe eines Kennworts (KeyStore-PIN) auffordert, geben Sie das Kennwort des Prüfadministrators ein.

   Die Ergebnisse werden auf der Standardausgabeeinheit angezeigt. Die Archivierungsdatei erhält die Erweiterung '.ixf'.

Informationen zur Befehlssyntax und Parameterbeschreibungen finden Sie im Abschnitt „Dienstprogramm Audit Archive and Sign" auf Seite 116.

Integrität der Datenbank des Prüfservers und der Archivierungsdateien prüfen

Tivoli PKI bietet ein Befehlszeilendienstprogramm, mit dem die Datenbank des Prüf-Servers und die archivierten Prüfdateien auf Manipulationen geprüft werden können. Dieses Tool trägt die Bezeichnung 'Audit Integrity Check'.

Anmerkung: Das Tivoli PKI-System muss vor der Ausführung dieses Dienstprogramms nicht heruntergefahren werden.

Mit diesem Dienstprogramm können Sie Manipulationen in den nachfolgenden Daten-Repositories lokalisieren. Sie werden in jedem Fall zur Eingabe des Kennworts für den Prüfadministrator [KeyStore-PIN] aufgefordert.

- Datenbank des Prüf-Servers
- Eine oder mehrere Prüf-Server-Archivierungsdateien
- Alle Archivierungsdateien in einem bestimmten Verzeichnis

Angenommen, Sie verwenden AIX und den Tivoli PKI-Standardpfad für Konfigurationsdateien. Melden Sie sich bei Tivoli PKI als Konfigurationsbenutzer (cfguser) an der Maschine an, auf der die Tivoli PKI-CA- und Prüf-Server-Komponente installiert ist. Sie möchten die nachfolgenden Komponenten nach Manipulationen durchsuchen.

- So prüfen Sie die Datenbank des Prüf-Servers:
  1. Geben Sie an der AIX-Befehlszeile folgenden Befehl ein:

     ```
     AuditIntegrityCheck -c /usr/lpp/iau/etc/TrustAuthority/
        AuditServer.ini -d
     ```

  2. Wenn das System Sie zur Eingabe eines Kennworts (KeyStore-PIN) auffordert, geben Sie das Kennwort des Prüfadministrators ein.

     Die Ergebnisse werden auf der Standardausgabeeinheit angezeigt.
- So prüfen Sie eine oder mehrere Archivierungsdateien des Prüf-Servers:
  1. Geben Sie an der AIX-Befehlszeile folgenden Befehl ein:

     ```
     AuditIntegrityCheck -c /usr/lpp/iau/etc/TrustAuthority/AuditServer.ini
         -a /usr/lpp/iau/arc/archive1_my.file
     ```

  2. Wenn das System Sie zur Eingabe eines Kennworts (KeyStore-PIN) auffordert, geben Sie das Kennwort des Prüfadministrators ein.

     Dieser Befehl prüft Dateien mit dem Pfadpräfix /usr/lpp/iau/arc/archive1_my.file und den Erweiterungen '.ixf' und '.sig'. Die Erweiterung '.ixf' kennzeichnet Dateien im von DB2 generierten Exportformat. Die Erweiterung '.sig' kennzeichnet eine vom Prüfsubsystem generierte Unterschriftsdatei.
- So prüfen Sie alle Archivierungsdateien in einem bestimmten Verzeichnis (in diesem Fall /usr/lpp/iau/arc/):
  1. Geben Sie an der AIX-Befehlszeile folgenden Befehl ein:

     ```
     AuditIntegrityCheck -c /usr/lpp/iau/etc/TrustAuthority/AuditServer.ini
         -A /usr/lpp/iau/arc/
     ```

  2. Wenn das System Sie zur Eingabe eines Kennworts (KeyStore-PIN) auffordert, geben Sie das Kennwort des Prüfadministrators ein.

     Dieser Befehl prüft im angegebenen Verzeichnis alle Dateien mit der Erweiterung '.ixf'.

Angenommen, Sie verwenden Windows NT und den Tivoli PKI-Standardpfad für Konfigurationsdateien. Melden Sie sich bei Tivoli PKI als Konfigurationsbenutzer an der Maschine an, auf der die Tivoli PKI-CA- und Prüf-Server-Komponente installiert ist. Sie möchten die nachfolgenden Komponenten nach Manipulationen durchsuchen.

- So prüfen Sie die Datenbank des Prüf-Servers:

  1. Geben Sie an der DOS-Eingabeaufforderung (in diesem Fall c:) folgenden Befehl ein:

     ```
     AuditIntegrityCheck -c "c:\Program Files\IBM\Trust Authority\etc\TrustAuthority\
        AuditServer.ini" -d
     ```

  2. Wenn das System Sie zur Eingabe eines Kennworts (KeyStore-PIN) auffordert, geben Sie das Kennwort des Prüfadministrators ein.

     Die Ergebnisse werden auf der Standardausgabeeinheit angezeigt.

- So prüfen Sie eine oder mehrere Archivierungsdateien des Prüf-Servers:

  1. Geben Sie an der DOS-Eingabeaufforderung (in diesem Fall c:) folgenden Befehl ein:

     ```
     AuditIntegrityCheck -c "c:\Program Files\IBM\Trust Authority\
        etc\TrustAuthority\AuditServer.ini" -a "c:\Program Files\IBM\Trust Authority\
        arc\archive1_meine.datei"
     ```

  2. Wenn das System Sie zur Eingabe eines Kennworts (KeyStore-PIN) auffordert, geben Sie das Kennwort des Prüfadministrators ein.

     Dieser Befehl prüft alle Dateien mit dem Pfadpräfix \Program Files\IBM\Trust Authority\arc\archive1_my.file und den Erweiterungen '.ixf' und '.sig'. Die Erweiterung '.ixf' kennzeichnet Dateien im von DB2 generierten Exportformat. Die Erweiterung '.sig' kennzeichnet eine vom Prüfsubsystem generierte Unterschriftsdatei. Die exportierten Dateien werden also unterzeichnet, und die Unterschrift wird in der Datei mit der Erweiterung '.sig' gespeichert.

- So prüfen Sie alle Archivierungsdateien in einem bestimmten Verzeichnis (in diesem Fall c:\Program Files\IBM\Trust Authority\arc\):

  1. Geben Sie an der DOS-Eingabeaufforderung (in diesem Fall c:) folgenden Befehl ein:

     ```
     AuditIntegrityCheck -c c:\Program Files\IBM\Trust Authority\etc\
          TrustAuthority\AuditServer.ini -A c:\Program Files\IBM\Trust Authority\arc\
     ```

  2. Wenn das System Sie zur Eingabe eines Kennworts (KeyStore-PIN) auffordert, geben Sie das Kennwort des Prüfadministrators ein.

     Dieser Befehl prüft im angegebenen Verzeichnis alle Dateien einschließlich der Dateien mit den Erweiterungen '.ixf' und '.sig'.

Informationen zur Befehlssyntax und Parameterbeschreibungen finden Sie im Abschnitt „Dienstprogramm Audit Integrity Check" auf Seite 116.

Status des Prüfservers prüfen

Je nach Umgebung können Sie den Status des Prüf-Servers mit folgenden Prozeduren prüfen:

- Unter AIX:
  1. Melden Sie sich bei AIX als Root an.
  2. Prüfen Sie die Prozesstabelle, und suchen Sie nach folgender Zeichenfolge:
     ```
     java
     ```
     Finden Sie diesen Prozess, fahren Sie mit Schritt 3 fort. Finden Sie diesen Prozess nicht, lesen Sie bitte im Abschnitt „Fehlerbehebung” auf Seite 135 nach.
  3. Wechseln Sie in das Verzeichnis 'bin'. Dieses Verzeichnis hat folgenden Standardpfad:
     ```
     /usr/lpp/iau/bin
     ```
  4. Prüfen Sie, ob der Port (in diesem Fall Port 59998) erfolgreich antwortet, indem Sie folgenden Befehl eingeben:
     ```
     ServerControl -i -c -k AUDIT -n
     Server -p 59998 -l
     "Protokolldatei"
     ```
     Hierbei steht *Server* für den Namen des Prüf-Servers, der mit dem angegebenen Port (in diesem Fall Port 59998) zugeordnet ist, und *Protokolldatei* für den Namen der Datei, in der die Ergebnisse des Befehls 'ServerControl' aufgezeichnet werden sollen.

     Ist die Antwort des geprüften Ports erfolgreich, wird folgende Nachricht angezeigt:
     ```
     Der Prüf-Server wird momentan ausgeführt.
     ```
     Hierbei steht *Server* für den Server, der Port 59998 zugeordnet ist.
- Unter Windows NT:
  1. Melden Sie sich bei Windows NT als Systemadministrator an.
  2. Starten Sie den Task-Manager durch Drücken der Tastenkombination **Strg**, **Alt** und **Entf**.
  3. Wählen Sie die Registerkarte **Prozesse** aus.
  4. Suchen Sie nach dem Prozess java.exe.

     Finden Sie diesen Prozess, fahren Sie mit Schritt 5 fort. Finden Sie diesen Prozess nicht, lesen Sie bitte im Abschnitt „Fehlerbehebung” auf Seite 135 nach.
  5. Wechseln Sie an der MS DOS-Eingabeaufforderung in das Verzeichnis 'bin'. Dieses Verzeichnis hat folgenden Standardpfad:
     ```
     c:\Program Files\IBM\Trust Authority\bin
     ```

6. Prüfen Sie, ob der Port (in diesem Fall Port 59998) erfolgreich antwortet, indem Sie folgenden Befehl eingeben:

   ServerControl -i -c -k AUDIT -n
   Server **-p 59998 -l**
   "*Protokolldatei***"**

   Hierbei steht *Server* für den Namen des Prüf-Servers, der Port 59998 zugeordnet ist, und *Protokolldatei* für den Namen der Datei, in der die Ergebnisse des Befehls 'ServerControl' aufgezeichnet werden sollen.

   Ist die Antwort des geprüften Ports erfolgreich, wird folgende Nachricht angezeigt:

   ```
   Der Prüf-Server wird momentan ausgeführt.
   ```

   Hierbei steht *Server* für den Server, der dem Tivoli PKI-Standard-Port 59998 zugeordnet ist.

Prüfserverprotokolle prüfen

Die Protokolle des Prüf-Servers zeichnen alle Transaktionen mit dem Prüf-Server auf. Sie können die Protokolle des Prüf-Servers an den nachfolgend beschriebenen Positionen prüfen.

Tabelle 7. Protokolle des Prüf-Servers

AIX-Standardpfad	Windows NT-Standardpfad	Beschreibung
/usr/lpp/iau/logs/smevents.log	c:\Program Files\IBM\Trust Authority\logs\smevents.log	Das Ereignisprotokoll des Prüf-Servers zur Aufzeichnung von Prüfereignissen.
/usr/lpp/iau/logs/iausmd.log	c:\Program Files\IBM\Trust Authority\logs\iausmd.log	Das Trace-Protokoll des Prüf-Servers zur Aufzeichnung von Programmaktivitäten.
/usr/lpp/iau/logs/iausmd.err	c:\Program Files\IBM\Trust Authority\logs\iausmd.err	Das Fehlerprotokoll des Prüf-Servers zur Aufzeichnung von Fehlernachrichten.

DB2-Datenbanken verwalten

In diesem Abschnitt werden grundlegende Prozeduren für Betrieb und Verwaltung von DB2-Datenbanken erläutert. Nähere Informationen hierzu finden Sie in der DB2 UDB-Dokumentation.

Tivoli PKI verwendet die in Tabelle 8 aufgeführten Datenbanken.

Tabelle 8. Datenbankpositionen

Exemplar	Datenbankname	Beschreibung
cfguser	cfgdb	Die Trust Authority-Standard-Konfigurationsdatenbank
cfguser	ibmdb	Die CA-Standarddatenbank
cfguser	pkrfdb	Die Standard-Registrierungsdatenbank
cfguser	adtdb	Die Standard-Prüfdatenbank
cfguser (AIX) ldapInst (Windows NT)	ldapdb	Die Standard-Directory-Datenbank bei einer Installation mit Tivoli PKI. Wenn Sie ein vorhandenes Verzeichnis verwenden, wird diese Position von Ihrem Unternehmen festgelegt.
cfguser	krbdb	Die Standarddatenbank für das Sichern und Wiederherstellen von Schlüsseln.

Status der DB2-Datenbanken prüfen

Je nach Umgebung können Sie den Status von DB2-Datenbanken mit folgenden Prozeduren prüfen:

- Unter AIX:
  1. Melden Sie sich bei AIX als Systemadministrator an.
  2. Geben Sie an der Eingabeaufforderung den Befehl **su** ein, um zum Konto des Benutzers mit Administratorberechtigung zu wechseln, der Tivoli PKI installiert hat.
  3. Geben Sie das Kennwort dieses Tivoli PKI-Benutzers ein.
  4. Geben Sie den folgenden Befehl ein:

     ```
     set DB2INSTANCE=Tivoli PKI_instance
     ```

     Hierbei steht *Tivoli PKI_instance* für die Benutzer-ID des Benutzers, der Tivoli PKI installiert hat.
  5. Geben Sie für die Standard-Konfigurationsdatenbank den Befehl **db2 connect to cfgdb** ein.

     Bei erfolgreicher Verbindung gibt das System folgende Nachricht zurück:

     ```
     Database server = DB2/6000 6.1.0
     SQL authorization ID = Tivoli PKI_instance
     Local database alias = cfgdb
     ```

6. Geben Sie für die Standard-CA-Datenbank den Befehl **db2 connect to ibmdb** ein.

   Bei erfolgreicher Verbindung gibt das System folgende Nachricht zurück:

   ```
   Database server = DB2/6000 6.1.0
   SQL authorization ID = Tivoli PKI_instance
   Local database alias = ibmdb
   ```

7. Geben Sie für die Standard-Registrierungsdatenbank den Befehl **db2 connect to pkrfdb** ein.

   Bei erfolgreicher Verbindung gibt das System folgende Nachricht zurück:

   ```
   Database server = DB2/6000 6.1.0
   SQL authorization ID = Tivoli PKI_instance
   Local database alias = pkrfdb
   ```

8. Geben Sie für die Standard-Prüfdatenbank den Befehl **db2 connect to adtdb** ein.

   Bei erfolgreicher Verbindung gibt das System folgende Nachricht zurück:

   ```
   Database server = DB2/6000 6.1.0
   SQL authorization ID = Tivoli PKI_instance
   Local database alias = adtdb
   ```

9. Geben Sie für die Standarddatenbank zur Schlüsselsicherung den Befehl **db2 connect to krbdb** ein.

   Bei erfolgreicher Verbindung gibt das System folgende Nachricht zurück:

   ```
   Database server = DB2/6000 6.1.0
   SQL authorization ID = Tivoli PKI_instance
   Local database alias = krbdb
   ```

10. Angenommen, die Standard-Directory-Datenbank wurde mit dem Produkt installiert. Geben Sie den Befehl **db2 connect to ldapdb** ein.

    Bei erfolgreicher Verbindung gibt das System folgende Nachricht zurück:

    ```
    Database server = DB2/6000 6.1.0
    SQL authorization ID = Tivoli PKI_instance
    Local database alias = ldapdb
    ```

11. Kehren Sie zum Root zurück.

- Unter Windows NT:

  1. Melden Sie sich bei Windows NT als Systemadministrator an.
  2. Starten Sie ein DB2-Befehlsfenster.
  3. Geben Sie den folgenden Befehl ein:

     set DB2INSTANCE=*Tivoli PKI_instance*

     Hierbei steht *Tivoli PKI_instance* für die Benutzer-ID des Benutzers, der Tivoli PKI installiert hat.

  4. Geben Sie für die Standard-Konfigurationsdatenbank den Befehl **db2 connect to cfgdb** ein.

     Bei erfolgreicher Verbindung gibt das System folgende Nachricht zurück:

     ```
     Database server = DB2/NT 6.1
     SQL authorization ID = Tivoli PKI_instance
     Local database alias = cfgdb
     ```

5. Geben Sie für die Standard-CA-Datenbank den Befehl **db2 connect to ibmdb** ein.

   Bei erfolgreicher Verbindung gibt das System folgende Nachricht zurück:

   ```
   Database server = DB2/NT 6.1
   SQL authorization ID = Tivoli PKI_instance
   Local database alias = ibmdb
   ```

6. Geben Sie für die Standard-Registrierungsdatenbank den Befehl **db2 connect to pkrfdb** ein.

   Bei erfolgreicher Verbindung gibt das System folgende Nachricht zurück:

   ```
   Database server = DB2/NT 6.1
   SQL authorization ID = Tivoli PKI_instance
   Local database alias = pkrfdb
   ```

7. Geben Sie für die Standard-Prüfdatenbank den Befehl **db2 connect to adtdb** ein.

   Bei erfolgreicher Verbindung gibt das System folgende Nachricht zurück:

   ```
   Database server = DB2/NT 6.1
   SQL authorization ID = Tivoli PKI_instance
   Local database alias = adtdb
   ```

8. Geben Sie den folgenden Befehl ein:

   set DB2INSTANCE=*ldap_Instance*

   Hierbei steht *ldap_Instance* für ldapInst, wenn das Directory zusammen mit dem Produkt installiert wurde.

9. Angenommen, die Standard-Directory-Datenbank wurde mit dem Produkt installiert. Geben Sie den Befehl **db2 connect to ldapInst** ein.

   Bei erfolgreicher Verbindung gibt das System folgende Nachricht zurück:

   ```
   Database server = DB2/NT 6.1
   SQL authorization ID = Tivoli PKI_instance
   Local database alias = ldapInst
   ```

10. Schließen Sie das DB2-Befehlsfenster.

DB2-Protokolle prüfen

Die DB2-Protokolle werden von Tivoli PKI im Hinblick auf den Systembetrieb nicht verwendet. Weitere Informationen zu den Protokollen finden Sie in der Dokumentation zu IBM DB2.

Directory-Server verwalten

In diesem Abschnitte werden grundlegende Prozeduren für Betrieb und Verwaltung von IBM Directory erläutert. Für einige dieser Verwaltungs-Tasks ist ein Kennwort erforderlich. Informationen zum Ändern des Kennworts für den Prüfadministrator finden Sie im Abschnitt „Tivoli PKI-Kennwörter ändern” auf Seite 5.

Dieser Directory-Server unterstützt LDAP-Standards (LDAP = Lightweight Directory Access Protocol). Er verfügt über eine DB2-Datenbank und befindet sich auf einer lokalen oder fernen Maschine. Bei diesem Server kann es sich um einen bereits vorhandenen oder einen speziell für Tivoli PKI installierten und konfigurierten Server handeln.

Weitere Informationen zur Interaktion von Tivoli PKI mit IBM Directory finden Sie im Handbuch *Tivoli PKI Konfiguration*.

Status des Directory-Servers prüfen

Je nach Umgebung können Sie den Status des Directory-Servers mit folgenden Prozeduren prüfen:

- Unter AIX:
  1. Melden Sie sich bei AIX als Root an.
  2. Prüfen Sie die Prozesstabelle, und suchen Sie nach folgender Zeichenfolge:
     ```
     slapd
     ```
     Finden Sie diesen Prozess, fahren Sie mit Schritt 3 fort. Finden Sie diesen Prozess nicht, lesen Sie bitte im Abschnitt „Fehlerbehebung” auf Seite 135 nach.
  3. Wechseln Sie in das Verzeichnis 'bin'. Dieses Verzeichnis hat folgenden Standardpfad:
     ```
     /usr/lpp/iau/bin
     ```
  4. Stellen Sie sicher, dass das Directory erfolgreich antwortet, und verwenden Sie hierzu folgenden Befehl:
     isdirup
     -h *server* **-a** *port* **-p** *installationspfad* **-t1 -f**
     /usr/lpp/iau/bin/

     Hierbei steht *server* für den Namen der Maschine, auf der das Directory ausgeführt wird, *port* für den Listener-Port des Directory-Servers und *installationspfad* für den Pfad, in dem das Directory installiert ist.

     Wenn die Antwort des Directory erfolgreich ist, enthält die Datei '/usr/lpp/iau/bin/isdirupStateValue' den Wert 0.
- Unter Windows NT:
  1. Melden Sie sich bei Windows NT als Systemadministrator an.
  2. Starten Sie den Task-Manager durch Drücken der Tastenkombination **Strg**, **Alt** und **Entf**.
  3. Wählen Sie die Registerkarte **Prozesse** aus.
  4. Suchen Sie nach dem Prozess slapd.exe.
     Finden Sie diesen Prozess, fahren Sie mit Schritt 5 fort. Finden Sie diesen Prozess nicht, lesen Sie bitte im Abschnitt „Fehlerbehebung” auf Seite 135 nach.
  5. Wechseln Sie an der MS DOS-Eingabeaufforderung in das Verzeichnis 'bin'. Dieses Verzeichnis hat folgenden Standardpfad:
     ```
     c:\Program Files\IBM\Trust Authority\bin
     ```

6. Stellen Sie sicher, dass das Directory erfolgreich antwortet, und verwenden Sie hierzu folgenden Befehl:

   ```
   isdirup -h server -a port -p
   installationspfad
   -tl
   ```

   Hierbei steht *server* für den Namen der Maschine, auf der das Directory ausgeführt wird, *port* für den Listener-Port des Directory-Servers und *installationspfad* für den Pfad, in dem das Directory installiert ist.

   Ist die Antwort des Directory erfolgreich, wird folgende Nachricht angezeigt:

   ```
   isdirup: returning: 0
   ```

Directory-Server-Protokolle prüfen

Sie können die Protokolle des Directory-Servers an den in Tabelle 9 angegebenen Positionen prüfen.

Tabelle 9. Protokolle des Directory-Servers

AIX-Standardpfad	Windows NT-Standardpfad	Beschreibung
/tmp/slapd.errors	c:*Directory-Installationspfad*\tmp\slapd.errors\	Fehlerprotokoll für das Directory.

IBM SecureWay 4758 PCI Cryptographic Coprocessor verwalten

Der IBM SecureWay 4758 PCI Cryptographic Coprocessor ist eine Tivoli PKI-Zusatzkomponente. Der IBM SecureWay 4758 PCI Cryptographic Coprocessor ist eine programmierbare PCI-Bus-Verschlüsselungskarte mit Manipulationsschutz, die DES- und RSA-Verschlüsselungsoperationen mit hoher Geschwindigkeit ermöglicht. In Tivoli PKI ist die Unterstützung für die Einheit IBM 4758 nur unter AIX verfügbar.

Sie können den Status des IBM SecureWay 4758 PCI Cryptographic Coprocessor mit dem Dienstprogramm csufcnm prüfen.

Der IBM SecureWay 4758 PCI Cryptographic Coprocessor erstellt keine Protokolle. Wenn bei der Einheit IBM 4758 ein Fehler auftritt, werden normalerweise ein Rückkehrcode und ein Ursachencode zusammen mit dem Fehler ausgegeben. Eine umfassende Liste mit den Rückkehr- und Ursachencodes sowie den zugehörigen Erläuterungen finden Sie im Handbuch *IBM 4758 CCA Basic Services Reference and Guide*. Diese Codes sind normalerweise ausreichend für eine vorläufige Fehlerbehebung.

Weitere Informationen finden Sie in der Dokumentation zum IBM SecureWay 4758 PCI Cryptographic Coprocessor.

4

Erläuterungen

Das vorliegende Kapitel liefert Ihnen Informationen, mit deren Hilfe Sie das Tivoli PKI-System effizient verwalten können. Die Abschnitte umfassen allgemeine Sicherheitsaspekte von Tivoli PKI sowie Informationen zu den Tivoli PKI-CAs (Zertifikatsaussteller), RAs (Registrierungsstellen) und zum Prüfsubsystem.

Tivoli PKI - Sicherheit

Das Sicherheits- und Sicherungsmodell von Tivoli PKI verfügt über die folgenden Merkmale:

- Codeunterzeichnung zur Absicherung der Software, die Operationen auf Schlüsselbasis durchführt.
- Verwendung von KeyStores zur Speicherung von und für den Zugriff auf Identitätsnachweise für Komponenten wie beispielsweise Schlüssel und Zertifikate. In den Komponenten-KeyStores gespeicherte Identitätsnachweise werden mit Hilfe eines Chiffrierschlüssels verschlüsselt, der von einem eingegebenen Kennwort abgeleitet wird.
- Zum Zwecke der Authentifizierung wird auch die Kommunikation zwischen Komponenten unterzeichnet. Hierzu zählen beispielsweise PKIX-Nachrichten zwischen der RA und dem CA.
- Für AIX-Systeme bietet Tivoli PKI einen hardwarebasierten Schutz von CA- und RA-Unterschriftsschlüsseln. Dies wird durch den Einsatz des optional verfügbaren IBM 4758 Cryptographic Coprocessor ermöglicht.

Zugriffssteuerungsliste (Access Control List - ACL)

Zugriffssteuerungslisten (ACL = Access Control Lists) bieten einen Mechanismus zur Einschränkung der Nutzung einer spezifischen Ressource auf berechtigte Benutzer. Zu den Tivoli PKI-Komponenten, die ACLs nutzen, zählen CA, RA und das Directory.

Der CA verwendet ACLs, um den Zugriff auf CA-Funktionen, wie beispielsweise die Erstellung von Zertifikaten, zu beschränken. Die RA verwendet ACLs, um den Zugriff auf RA-Funktionen, wie beispielsweise die Genehmigung von Anforderungen, zu beschränken. Das Directory nutzt ACLs, um den Zugriff auf verschiedene Directory-Bereiche zu begrenzen, die möglicherweise sensible Informationen enthalten.

Zertifikatsaussteller (Certification Authority - CA)

Ein Zertifikatsaussteller (CA = Certificate Authority) ist die Entität, die für die Einhaltung der Sicherheitsregeln eines Unternehmens verantwortlich ist und sichere elektronische Identitäten in Form von Zertifikaten zuweist. Die mit dem privaten Schlüssel des CA unterzeichneten Zertifikate enthalten Identifikations- und andere Informationen zum Eigentümer des Zertifikats.

Der Tivoli PKI-CA hat folgende Aufgaben:

- Verarbeitung von Ausstellungs-, Erneuerungs- oder Widerrufanforderungen der RAs.
- Verwaltung einer Zugriffssteuerungsliste (ACL), die durch Dateiberechtigungen geschützt ist. Diese Liste enthält die registrierten Namen (DNs) berechtigter RAs und Administratoren.
- Verwaltung einer Liste der ausgestellten Zertifikate (ICL = Issued Certificates List) in der CA-Datenbank. Diese Liste enthält Informationen zum Zertifikatstatus, zur Seriennummer sowie CRL-Informationen.

  Der CA leitet ICL-Informationen an die Tivoli PKI-RA weiter, die wiederum Zertifikate und CRLs im Directory publiziert.

  In der CA-Datenbank gespeicherte Sätze verwenden zum Schutz einen Nachrichtenauthentifizierungscode (MAC = Message Authentication Code). Die Prüfung dieser Sätze ist eine Tivoli PKI-Option mit der Bezeichnung Integritätsprüfung.
- Speicherung der eigenen Schlüssel und Zertifikate im Tivoli PKI-KeyStore.
- Generierung von Prüfsätzen für sicherheitsrelevante Ereignisse und deren Weiterleitung an den Prüf-Server.
- Unterstützung von gegenseitiger Zertifizierung und CA-Hierarchien.
- Unterstützung der Generierung und Bestätigung von Zertifikaten, die benutzerdefinierte und vom Benutzer ausgewählte Zertifikatserweiterungen enthalten.

CA-Hierarchien

Eine CA-Hierarchie ist eine Sicherungsstruktur, bei der sich ein CA an der Spitze dieser Struktur befindet. Dieser Spitze können bis zu vier CA-Ebenen untergeordnet sein. Werden Benutzer oder Server bei einem CA registriert, erhalten sie ein Zertifikat, das von diesem CA unterzeichnet wurde. Auf diese Weise übernehmen sie die Zertifizierungshierarchie der darüberliegenden Ebenen. In Tivoli PKI kann ein CA als Teil einer internen, einer Abwärts- oder einer Aufwärtshierarchie konfiguriert werden. Die einzelnen Hierarchietypen sind wie folgt definiert:

Interne Hierarchie

Eine interne Hierarchie besteht ausschließlich aus Tivoli PKI-CAs. CAs in einer solchen Hierarchie verwenden das PKIX-Protokoll CMP (Certificate Messaging Protocol).

Aufwärtshierarchie

Eine Aufwärtshierarchie ist definiert als die Kombination aus einem oder mehreren Tivoli PKI-CAs und einem oder mehreren Fremd-CAs. Hierbei befinden sich die Tivoli PKI-CAs in der Trust-Kette unter den Fremd-CAs. Daher wird die Hierarchie vom Tivoli PKI-CA aus aufwärts betrachtet. In einer solchen Hierarchie verwenden die CAs die Protokolle PKCS#7 und PKCS#10.

Abwärtshierarchie

Eine Abwärtshierarchie ist definiert als die Kombination aus einem oder mehreren Tivoli PKI-CAs und einem oder mehreren Fremd-CAs. Hierbei befinden sich die Tivoli PKI-CAs in der Trust-Kette über den Fremd-CAs. Daher wird die Hierarchie vom Tivoli PKI-CA aus abwärts betrachtet. In einer solchen Hierarchie verwenden die CAs die Protokolle PKCS#7 und PKCS#10.

CAs können technisch gesehen in der Mitte einer Hierarchie stehen, die sowohl über als auch unter dem Tivoli PKI-CA Fremd-CAs Der Tivoli PKI-CA kann auch als sich selbst unterzeichnender CA konfiguriert sein. In diesem Fall ist der CA nicht Bestandteil einer Hierarchie.

Tivoli PKI unterstützt eine hierarchische Zertifizierung zwischen CAs, die das PKIX-CMP-Protokoll sowie die Protokolle PKCS#7 und PKCS#10 einhalten. Tivoli PKI unterstützt außerdem eine Hierarchie mit Fremd-CAs, die die Protokolle PKCS#7 und PKCS#10 verwenden.

Zertifikatserweiterungen

Die X.509v3-Zertifikatserweiterungen bieten Methoden zur Zuordnung weiterer Attribute zu Benutzern oder öffentlichen Schlüsseln und zur Verwaltung der CA-Hierarchie. Das X.509v3-Format ermöglicht Benutzergemeinschaften außerdem, private oder allgemeine Erweiterungen zu definieren, die spezifische Informationen für diese Gemeinschaft enthalten.

Jede Erweiterung eines Zertifikats kann als kritisch oder unkritisch gekennzeichnet werden. Ein System, das Zertifikate im X.509v3-Format nutzt, muss ein Zertifikat zurückweisen, wenn dieses eine kritische Erweiterung enthält, die dem System nicht bekannt ist. Eine unbekannte unkritische Erweiterung kann jedoch ignoriert werden.

Es gibt drei Arten von Zertifikatserweiterungen:

- Standarderweiterungen
- Allgemeine Erweiterungen
- Private Erweiterungen

Standarderweiterungen

Eine Zertifikatsstandarderweiterung ist eine Erweiterung, deren Bedeutung und Syntax im ITU-Standard RFC 2459 definiert ist. Bis auf eine sind alle diese Erweiterungen auch in X.509v3 definiert. Einige von ihnen sind nur innerhalb von CA-Zertifikaten definiert. Tivoli PKI ermöglicht das Hinzufügen der meisten Standarderweiterungen zu einem Zertifikat (hierfür gelten die in Tabelle 10 dargestellten Regeln):

Tabelle 10. Zertifikatserweiterungen

Erweiterung	Beschreibung
Schlüsselverwendung	Diese Erweiterung gibt den Zweck der Verwendung des zertifizierten öffentlichen Schlüssels an. Die Einstellungen werden in der Regel durch Zertifizierungsschablonen definiert.
Alternativer Name des Zertifikatsgegenstands	Diese Erweiterung enthält einen oder mehrere Alternativnamen in verschiedenen Namensformaten für die Entität, die vom CA dem zertifizierten öffentlichen Schlüssel zugeordnet wurde. In der Regel wird in Zertifizierungsschablonen definiert, welche dieser Namensformate in Zertifikaten verwendet werden dürfen, die diese Schablone nutzen.

Tabelle 10. Zertifikatserweiterungen (Forts.)

Erweiterung	Beschreibung
Schlüsselkennung des Zertifikatsgegenstands	Diese Erweiterung legt fest, welcher öffentliche Schlüssel durch ein bestimmtes Zertifikat zertifiziert wird. Diese Erweiterung dient primär der Unterscheidung von Schlüsseln, wenn mehrere Schlüssel für eine Entität zertifiziert sind oder zertifiziert wurden. Der Wert dieser Erweiterung wird in Tivoli PKI immer vom CA definiert.
Schlüsselkennung des Ausstellers	Diese Erweiterung gibt an, welcher öffentliche Schlüssel vom Aussteller eines Zertifikats zu dessen Unterzeichnung verwendet wurde. Diese Erweiterung dient primär der Unterscheidung von Schlüsseln, wenn mehrere Schlüssel für einen Aussteller zertifiziert werden. Der Wert dieser Erweiterung wird immer vom CA definiert.
Nutzungszeitraum für privaten Schlüssel	Diese Erweiterung schränkt die Nutzung des privaten Schlüssels gemäß der Gültigkeitsdauer des Zertifikats ein. Das aktuelle PKIX-Zertifikatsprofil RFC 2459 gibt an, dass die Nutzung dieses Schlüssels nicht länger empfohlen wird.
Erweiterung von Zertifizierungsregeln	Diese Erweiterung enthält eine Reihe von Regelanzeigern. Ein solcher Anzeiger kann beispielsweise eine Objektkennung sein, deren Bedeutung publiziert werden muss. Es kann sich jedoch auch um eine Objektkennung in Verbindung mit einer Beschreibung der angestrebten Regel handeln. Die Beschreibung der Regel kann durch eine Webadresse angegeben sein, unter der sie abgerufen werden kann, oder aber durch einen kurzen Text, der in das Zertifikat aufgenommen wird.
Alternativname des Ausstellers	Diese Erweiterung enthält einen oder mehrere Alternativnamen in verschiedenen Namensformaten für den Aussteller des Zertifikats. Der Wert dieser Erweiterung wird immer vom CA definiert.
Directory-Attribute des Zertifikatsgegenstands	Diese Erweiterung enthält eine Reihe zusätzlicher Directory-Attribute des Zertifikatsgegenstands, die nicht Teil des registrierten Namens sind. Diese Erweiterung muss als unkritisch definiert werden.
Erweiterte Schlüsselverwendung	Diese Erweiterung enthält eine Reihe von Objektkennungen, die den Nutzungszweck für den zertifizierten öffentlichen Schlüssel angeben. Die Einstellungen werden in der Regel durch Zertifizierungsschablonen definiert. Die Werte dieser Erweiterung können durch eine Benutzergemeinschaft definiert oder von RFC 2459 abgeleitet werden.
Grundlegende Einschränkungen	Diese Erweiterung ist nur bei CA-Zertifikaten sinnvoll. Sie ist in allen CA-Zertifikaten enthalten, die von Tivoli PKI erstellt wurden. Bei allen anderen Zertifikaten ist diese Erweiterung entweder nicht vorhanden oder leer. RFC 2459 empfiehlt, diese Erweiterung nicht leer- sondern wegzulassen. Diese Erweiterung kennzeichnet ein Zertifikat nicht nur als CA-Zertifikat, sondern kann auch den Zertifizierungspfad mit maximaler Länge enthalten. Auf diese Weise kann definiert werden, wie viele zusätzliche CA-Ebenen durch diesen CA zertifiziert werden können. Diese Erweiterung muss als kritisch definiert werden.

Tabelle 10. Zertifikatserweiterungen (Forts.)

Erweiterung	Beschreibung
Namenseinschränkungen	Diese Erweiterung wird nur in CA-Zertifikaten verwendet. Sie definiert einen Namensbereich, in dem sich alle Namen und Alternativnamen des Zertifikatsgegenstands befinden müssen, sofern es sich um Zertifikate handelt, die vom CA mit diesem Zertifikat oder von untergeordneten CAs ausgestellt wurden. Der Zweck dieser Erweiterung ist die Einschränkung von Namen, die von Zertifikaten in diesem Zertifizierungspfad genutzt werden können. Einschränkungen werden in Form von Unterverzeichnisstrukturen für zulässige oder nicht zulässige Namen definiert. Ein Name, der einer Beschränkung in einer Unterverzeichnisstruktur nicht zulässiger Namen entspricht, ist ungültig, unabhängig von den Informationen in der Unterverzeichnisstruktur der zulässigen Namen. Diese Erweiterung muss als kritisch definiert werden.
Regelzuordnung	Diese Erweiterung wird nur in CA-Zertifikaten verwendet. Tivoli PKI definiert diese Erweiterung nicht in Zertifikaten, für die es die ursprüngliche Anforderung erstellt hat.
Regeleinschränkungen	Diese nur in CA-Zertifikaten verwendete Erweiterung kann für einen der folgenden Zwecke eingesetzt werden: Sie kann das Zuordnen von Regeln in Zertifikaten des aktuellen Zertifizierungspfads verhindern oder für diese Zertifikate spezifische Regeln erforderlich machen.
CRL-Verteilungspunkte	Diese Erweiterung gibt an, wo sich eine partielle CRL mit Widerrufinformationen zum aktuellen Zertifikat befindet. Sie wird gesetzt, wenn ein gültiger Wert ungleich Null für den Parameter 'certPerDP' in der Datei 'jonahca.ini' angegeben wird.
Informationszugriff für Aussteller	Diese Erweiterung gibt an, wo und wie auf bestimmte Informationen zum Aussteller des Zertifikats mit dieser Erweiterung zugegriffen werden kann. Diese Erweiterung ist derzeit in von Tivoli PKI erstellten Zertifikaten nicht definiert.

Allgemeine Erweiterungen

Tivoli PKI definiert eine einzelne, vom Standard abweichende Erweiterung als allgemeine Erweiterung. Diese Erweiterung kann von jedem Unternehmen eingesetzt werden, die Tivoli PKI nutzt. Es handelt sich hierbei um die Erweiterung für die Zuordnung der Host-Identität, die den Zertifikatsgegenstand einer entsprechenden Identität auf einem Host-System zuweist.

Private Erweiterungen

Jede für die Nutzung von Tivoli PKI ausgelegte Client-Anwendung kann eine Erweiterung definieren, deren Identität und Syntax entweder der Anwendung privat zur Verfügung stehen oder in einer Benutzergemeinschaft gemeinsam genutzt werden. Diese Erweiterungen müssen als unkritisch definiert werden. Wird die Erweiterung zum ersten Mal definiert, muss ihr eine Objektkennung zugewiesen werden. Außerdem müssen Sie sie gemäß ITU-Standard X.660 und ISO-Standard 9834-1 (identisch) registrieren. Dies gilt auch für die Syntax.

Ablauf der Erweiterungsanforderung

Erweiterungen können von einem Benutzer angefordert werden, Sie müssen jedoch vom CA oder einer RA, die als CA dient, bestätigt werden. Dieser Prozess läuft wie folgt ab:

1. Der Benutzer fordert eine Erweiterung an und übermittelt die dazu erforderlichen Informationen, einschließlich einer eindeutigen Erweiterungskennung und eines Werts. Der Benutzer definiert, ob es sich um eine kritische Erweiterung handelt.
2. Die Erweiterungsanforderung und die Informationen werden in die Zertifikatsanforderung an die RA aufgenommen.
3. RA oder CA prüfen bei der Verarbeitung der Zertifikatsanforderung, ob die Erweiterung den Zertifizierungsregeln der Unternehmen entspricht. Die Erweiterungsanforderung wird dementsprechend geändert oder außer Kraft gesetzt. Nach Prüfung der Erweiterung wird diese vom CA zertifiziert.

Zertifikatswiderrufsliste (CRL)

Eine Zertifikatswiderrufsliste (CRL) ist eine digital unterzeichnete, mit Zeitmarken versehene Liste der Zertifikate, die vom Zertifikatsaussteller (CA) widerrufen wurden. Die Zertifikate in dieser Liste sollten als nicht akzeptierbar behandelt werden.

Zertifikate können widerrufen werden, wenn ihre Gültigkeit abgelaufen oder ihre Sicherheit fraglich ist. Der Status eines Zertifikats wird in der ICL geändert. Zur festgelegten Zeit erstellt der CA die CRL mit der Seriennummer und dem CA-DN des Ausstellers des widerrufenen Zertifikats. Obwohl bei einem Widerruf das entsprechende Zertifikat und dessen Informationen in der ICL geändert werden, ist ein Widerruf erst dann endgültig, wenn die CRL ausgegeben und im Directory publiziert wird.

In Tivoli PKI werden die Gültigkeitsdauer einer publizierten CRL und der Zeitraum zwischen CRL-Publizierungen in der CA-Konfigurationsdatei 'jonahca.ini' definiert und geändert.

Sie können auch CRL-Verteilungspunkte nutzen, um die Anzahl der CRLs, die nacheinander verarbeitet werden sollen, zu definieren und zu partitionieren. Statt eine immer größere Anzahl widerrufener Zertifikate an einer Position bzw. unter einem einzelnen Eintrag im Directory-Server zu akkumulieren, können Sie die Liste der widerrufenen Zertifikate auf mehrere Verteilungspunkte aufteilen. Sie aktivieren diese Funktion, indem Sie den Parameter 'certPerDp' in der Konfigurationsdatei 'jonahca.ini' entsprechend einstellen.

Gegenseitige Zertifizierung

Bei der gegenseitigen Zertifizierung handelt es sich um ein Sicherungsmodell, in dem ein Zertifikat, das einen öffentlichen CA-Schlüssel enthält, der einem entsprechenden privaten CA-Unterschriftsschlüssel für das Ausstellen von Zertifikaten zugeordnet ist, von einem CA an einen anderen CA ausgestellt wird. Typischerweise wird die gegenseitige Zertifizierung eingesetzt, um Client-Systemen oder Endentitäten in einer Registrierungsdomäne die sichere Kommunikation mit Client-Systemen oder Endentitäten in einer anderen Registrierungsdomäne zu ermöglichen.

Obwohl die gegenseitige Zertifizierung zwischen CAs in beiden Richtungen erfolgen kann, werden in Tivoli PKI Anforderungen für die gegenseitige Zertifizierung nur in einer Richtung unterstützt. Die gegenseitige Zertifizierung in beiden Richtungen ist möglich, wenn jeder CA ein gegenseitiges Zertifikat vom jeweils anderen CA erhält. Tivoli PKI unterstützt eine gegenseitige Zertifizierung nur zwischen CAs, die das PKIX-CMP-Protokoll einhalten.

Zertifizierung

Als Zertifizierung bezeichnet man die Erstellung eines digitalen Zertifikats für eine Entität oder eine Person. In Tivoli PKI erfolgt die Zertifizierung nur nach Prüfung und Bestätigung einer Zertifizierungsanforderung durch die RA. Als Ergebnis der Registrierung stellt der CA die entsprechenden Zertifikate aus.

Digitale Zertifikate

Ein digitales Zertifikat ist ein elektronischer Identitätsnachweis, der einer Person oder einer Entität von einem vertrauenswürdigen Dritten ausgestellt wird. Jedes Zertifikat ist mit dem privaten Schlüssel des CA unterzeichnet. Es bürgt für die Identität einer Person, eines Unternehmens oder einer Organisation.

Abhängig vom Aufgabenbereich des CA kann das Zertifikat den Identitätsnachweis seines Eigners bestätigen, e-Business über das Internet ausführen zu dürfen. In gewissem Sinne entspricht ein digitales Zertifikat einem Führerschein oder einem medizinischen Diplom. Es bestätigt, dass der Eigner des entsprechenden privaten Schlüssels berechtigt ist, bestimmte e-Business-Aktivitäten auszuführen.

Ein Zertifikat enthält Informationen über die Entität, die von ihm zertifiziert wird, gibt an, ob es sich um eine Person, eine Maschine oder ein Computerprogramm handelt, und enthält als Teil dieser Informationen den zertifizierten öffentlichen Schlüssel dieser Entität.

Bei Tivoli PKI entspricht der Typ des ausgestellten Zertifikats den geschäftlichen Regeln Ihres Unternehmens.

Registrierte Namen

Ein registrierter Name (DN = Distinguished Name) ist der eindeutige Name eines im Directory gespeicherten Datensatzes. Der DN kennzeichnet eindeutig die Position eines Datensatzes in der hierarchischen Struktur des Directory. Diese Struktur wird auch als Directory Information Tree (DIT) bezeichnet.

Die Struktur verfügt über einen einzigen Stamm und eine unbegrenzte Anzahl von Knoten, die sich vom Stamm verzweigen. Jeder Knoten entspricht einem durch Attribute gekennzeichneten Directory-Eintrag. Die Beschreibung eines DNs für einen Directory-Eintrag hängt von den Syntaxanforderungen des Directory-Clients und dem Zugriffsprotokoll des Directory-Servers ab.

In Tivoli PKI, das auf IBM Directory basiert, kann ein DN für einen Directory-Eintrag wie folgt aussehen:

```
/C=US/O=IBM/OU=Tivoli PKI/MAIL=cjsmith@vnet.ibm.com,CN=Chris Smith
```

Hierbei steht US für das Land (C), IBM für das Unternehmen (O), Tivoli PKI für die Abteilung innerhalb des Unternehmens (OU), cjsmith@vnet.ibm.com für die E-Mail-Adresse (MAIL) und Chris Smith für den allgemeinen Namen (CN).

Liste der ausgestellten Zertifikate (ICL)

Die Liste der ausgestellten Zertifikate (ICL = Issued Certificates List) ist eine vollständige Liste der Zertifikate (einschließlich deren Status), die von einem CA ausgestellt wurden. Die Zertifikate sind nach Seriennummer und Status indexiert. Die ICL wird vom CA verwaltet und in der CA-Datenbank gespeichert. Diese Liste dient zur Ermittlung der Zertifikate, die in einer Zertifikatwiderrufsliste (CRL = Certificate Revocation List) publiziert werden sollten.

Die Tivoli PKI-ICL verfügt über folgende Merkmale:

- ODBC-Implementierung (Open Database Connectivity, in Tivoli PKI über DB2)
- Optionale Verwendung von MACs in Datenbankeinträgen zur Gewährleistung der Integrität (nur ODBC)
- Verschleierung von Chiffrier- und MAC-Schlüssel zur Laufzeit
- Unterstützung mehrerer Verbindungen (pro Thread) mit einem standardmäßigen Maximalwert
- Zugriff auf die Prüfprotokollfunktion

Unterzeichnen und Gültigkeitsprüfung für Unterschriften

Als Unterzeichnen wird die Verwendung eines privaten Schlüssels zum Generieren einer Unterschrift bezeichnet. Eine Gültigkeitsprüfung beinhaltet die Verwendung des entsprechenden öffentlichen Schlüssels zur Bestätigung der Unterschrift.

Tivoli PKI verwendet zur Unterzeichnung und für Gültigkeitsprüfungen eine Verschlüsselungsmaschine auf PKIX-Basis. Dieses Produkt ermöglicht es Anwendungen, Informationen zu ver- und entschlüsseln. Mit diesem Produkt können Anwendungen eine digitale Unterschrift prüfen, ein Zertifikat von einem Directory abrufen und entscheiden, ob ein Zertifikat gesichert ist. Diese Verschlüsselungsmaschine bietet außerdem nahtlose Unterstützung für die hardwaregestützte Verschlüsselung. Sie unterstützt den IBM SecureWay 4758 PCI Cryptographic Coprocessor oder jedes andere Hardware-Token mit PKCS#11-Schnittstelle.

Alle Tivoli PKI-Softwarekomponenten, die Verschlüsselungs- und KeyStore-Operationen durchführen, werden von dieser Verschlüsselungsmaschine unterzeichnet.

Registrierungsstellen (RA)

Eine Registrierungsstelle (RA = Registration Authority) ist ein Server-Prozess, der die administrativen Aufgaben im Bereich der digitalen Zertifizierung übernimmt. In Tivoli PKI kann eine RA Anforderungen genehmigen oder zurückweisen sowie den Widerruf eines Zertifikats einleiten. Die RA gewährleistet, dass die geschäftlichen und Zertifizierungsregeln eines Unternehmens eingehalten werden.

Registratoren

Registratoren können über den Tivoli PKI RA Desktop Verwaltungs-Tasks für Registrierungsanforderungen ausführen. Damit ein Registrator diese Tasks ausführen kann, muss die entsprechende Person als Registrator registriert werden. Anweisungen zur Registrierung eines Registrators finden Sie unter „Registrator hinzufügen” auf Seite 37.

Über den RA Desktop können Registratoren folgende Statuswerte von Zertifikatsanforderungen abrufen: Empfangen, Anstehend, Genehmigt, Nicht genehmigt, Abgeschlossen. Zu den weiteren Abfragefeldern des RA Desktop zählen Vor- und Nachname, Aktualisierungsdatum, Erstellungsdatum und Ablaufdatum des Zertifikats. Zeigt der RA Desktop die zu einer Abfrage gefundenen Einträge in Tabellenform an, kann der Registrator für die Ergebnisse weitere Maßnahmen ergreifen. So kann er beispielsweise eine Registrierungsanforderung bestätigen oder zurückweisen oder den Erneuerungsstatus eines Zertifikats widerrufen oder ändern.

Registrierungsdomänen

Eine Registrierungsdomäne ist eine Gruppe von Ressourcen, Regeln und Konfigurationsoptionen, die sich auf bestimmte Registrierungsprozesse für Zertifikate beziehen. Der Domänenname ist eine Untergruppe der Webadresse, die zum Widerrufen von Registrierungsoperationen verwendet wird. Sie dient als eindeutige Unterzeichnung der Anwendung. Tivoli PKI unterstützt eine Registrierungsdomäne pro Tivoli PKI-Installation.

Mehrere RAs

Tivoli PKI unterstützt mehrere RAs (MRAs). Bei der Installation von Tivoli PKI wird sowohl ein erster CA als auch eine erste RA installiert. Durch die Unterstützung von mehrere RAs wird es möglich, mehrere RAs unter einem CA zu installieren. Dank dieser Funktion können Sie verschiedene RA-Server für unterschiedliche Zwecke definieren. Eine Situation, in der dies erforderlich sein könnte, wäre beispielsweise eine Muttergesellschaft, die für ihre einzelnen Tochtergesellschaften unterschiedliche Zertifikattypen ausstellen muss. Dies wird durch die Einrichtung mehrerer RAs möglich. Jede RA verwendet denselben CA, kann jedoch Zertifikate anhand unterschiedlicher Regeln ausstellen. Anweisungen zur Einrichtung von mehreren RAs finden Sie unter „Mehrere RAs installieren” auf Seite 44.

Übergabe der Trust-Kette

Die Übergabe der Trust-Kette ist das Konzept, bei dem die gesamte Trust-Hierarchie eines CA für jedes Zertifikat übergeben wird, das über eine RA ausgestellt wird. Wird die Trust-Kette nicht übergeben, werden neue Zertifikate zwar durch einen CA unterzeichnet, aber das Zertifikat enthält in diesem Fall keine Angaben über die Hierarchie dieses CA. Daher kann bei der Berechtigung des Zertifikats lediglich die Tatsache ermittelt werden, dass das Zertifikat durch diesen CA unterzeichnet wurde. Bei einer Übergabe der Trust-Kette enthält hingegen jedes ausgestellte Zertifikat die gesamte Trust-Hierarchie des unterzeichnenden CA. Auf diese Weise kann das Zertifikat in der gesamten Hierarchie des CA berechtigt werden. Die Übergabe der Trust-Kette kann je nach den Anforderungen des Administrators aktiviert oder inaktiviert werden. Weitere Informationen dazu, wie Sie die Übergabe der Trust-Kette aktivieren bzw. inaktivieren, finden Sie unter „Übergabe der Trust-Kette aktivieren bzw. inaktivieren” auf Seite 43.

Wenn die Übergabe der Trust-Kette aktiviert ist, werden Trust-Ketten an den ein Zertifikat Anfordernden übergeben, sobald ein Zertifikat ausgestellt wird. Die Trust-Kette muss ein Mal für jeden Browser oder Server heruntergeladen werden.

IBM SecureWay 4758 PCI Cryptographic Coprocessor

Der IBM SecureWay 4758 PCI Cryptographic Coprocessor ist eine programmierbare PCI-Bus-Verschlüsselungskarte mit Manipulationsschutz, die zur Gewährleistung der Vertraulichkeit und Integrität des Unterschriftsschlüssels Ihres Unternehmens beiträgt. Diese Hardware wird auch als Hardwaresicherheitsmodul (Hardware Security Module - HSM) bezeichnet. Diese Karte verwendet die API der IBM Common Cryptographic Architecture (CCA) und stellt umfassende Verschlüsselungsservices, einschließlich DES- und RSA-Verschlüsselung, zur Verfügung. DES und RSA sind die am weitesten verbreiteten Algorithmen für kommerzielle Verschlüsselungssysteme. Aufgrund der Leistungsfähigkeit dieser Algorithmen sollten Sie den von Ihnen verwendeten Methoden zur Schlüsselverwaltung besondere Aufmerksamkeit zukommen lassen. Ist die Vertraulichkeit eines Schlüssels nicht mehr gewährleistet, können unter Umständen Unbefugte auf die mit diesem Schlüssel verschlüsselten Daten zugreifen. Der IBM SecureWay 4758 PCI Cryptographic Coprocessor ermöglicht mit folgenden Merkmalen die Erweiterung des umfassenden Schutzes für diese Schlüssel:

- Dreifache Verschlüsselung von Schlüsseln mit Hilfe eines speziellen, in der dedizierten Hardware gespeicherten Schlüssels
- Schutz von Endpunkt-zu-Endpunkt-Datenübertragungen
- Programmatisches Definieren von änderbaren Regeln und Profilen
- Nutzung eines Zufallsgenerators auf Hardwarebasis zur Erstellung nicht vorausberechenbarer Schlüssel

Die Verschlüsselungsprozesse finden in einem sicheren und abgegrenzten Bereich auf der Karte statt. Die Karte ist so ausgelegt, dass sie den strengen Anforderungen des Standards FIPS PUB 140-1 Stufe 4 entspricht. Innerhalb des sicheren Bereichs kann Software ausgeführt werden.

In Tivoli PKI ermöglicht der IBM SecureWay 4758 PCI Cryptographic Coprocessor die Generierung von CA- und RA-Unterschriftsschlüsseln. Die durch den IBM SecureWay 4758 PCI Cryptographic Coprocessor erstellten Schlüssel werden durch die Karte geschützt, indem sie mit dem 4758-Hauptschlüssel verschlüsselt werden. Die CA- und RA-Schlüssel können entweder im Schlüsselspeicher (KeyStore) oder im IBM SecureWay 4758 PCI Cryptographic Coprocessor gespeichert werden.

Der IBM SecureWay 4758 PCI Cryptographic Coprocessor ist eine optionale, aber empfohlene Tivoli PKI-Komponente, die nur für die AIX-Plattform verfügbar ist. Zudem handelt es sich beim IBM 4758 Cryptographic Coprocessor um ein separates und äußerst komplexes Produkt. Daher sollten Sie mit seiner Dokumentation und den entsprechenden Prozeduren vertraut sein. Am Ende dieses Abschnitts finden Sie eine Liste der empfohlenen Literatur.

Zusätzliche Informationen zum IBM SecureWay 4758 PCI Cryptographic Coprocessor sind unter der folgenden Webadresse verfügbar:

`http://www.ibm.com/security/cryptocards/`

Unterschiede zwischen den Optionen für Beibehaltung und Nicht-Beibehaltung

Eine der Entscheidungen, die der Administrator einer durch einen IBM 4758 Cryptographic Coprocessor erweiterten Tivoli PKI-Installation treffen muss, ist die Verwendung der Option für die Beibehaltung (’retain’). Die Fähigkeit, sensible private Schlüssel im gesicherten integrierten Speicher beizubehalten, ist eine der leistungsstärksten Funktionen des IBM 4758 Cryptographic Coprocessor und kann die Vertraulichkeit des CA- und RA-Schlüssels vergrößern. Da dieser Speicher jedoch speziell dazu entwickelt wurde, Kopiervorgänge zu verhindern, ist die Erstellung einer Sicherungskopie der beibehaltenen privaten Schlüssel nicht möglich.

Sowohl bei der Beibehaltung als auch bei der Nicht-Beibehaltung (’Non-retain’) werden die privaten Unterschriftsschlüssel zu keinem Zeitpunkt außerhalb der sicheren Grenzen der geschützten integrierten Verarbeitungsumgebung des IBM 4758 Cryptographic Coprocessor preisgegeben. In einer Installation, bei der die Option für die Beibehaltung eingesetzt wird, wird der private Schlüssel stets innerhalb des IBM 4758 Cryptographic Coprocessor erstellt sowie physisch gespeichert und kann nicht aus diesem entfernt werden. Verwendet eine Installation die Option für die Nicht-Beibehaltung, wird der private Schlüssel auch hier innerhalb der geschützten Umgebung des IBM 4758 Cryptographic Coprocessor erstellt, jedoch außerhalb des IBM 4758 Cryptographic Coprocessor in einer stark verschlüsselten Form gespeichert, auf die nur ein IBM 4758 Cryptographic Coprocessor mit Hilfe des

Hauptschlüssels zugreifen kann. Bei dieser Option stellt der IBM 4758 Cryptographic Coprocessor den verschlüsselten privaten Schlüssel in die gesicherte Umgebung, entschlüsselt ihn unter Verwendung des Hauptschlüssels und führt dann die angeforderte Operation aus.

Neben der offensichtlichen Sicherheitsfunktionalität gibt es hinsichtlich der Sicherung einen weiteren wichtigen Unterschied zwischen den beiden Installationsoptionen. Unter gesteuerten Bedingungen lässt der IBM 4758 Cryptographic Coprocessor die Erstellung von mehreren IBM 4758 Cryptographic Coprocessor als 'Klone' zu. Jeder dieser Klone verwendet denselben Hauptschlüssel und kann daher einen gemeinsamen Zugriff auf 'nicht beibehaltene' Schlüssel verwenden. Bei der Prozedur zum Klonen des IBM 4758 Cryptographic Coprocessor wird nur der Hauptschlüssel zwischen den einzelnen Einheiten übertragen. Wie bei jeder anderen Prozedur ist es auch hier nicht möglich, auf den Speicher zuzugreifen, der für beibehaltene Schlüsseldaten verwendet wird. Der gesicherte integrierte Speicher für beibehaltene Schlüssel ist so konzipiert, dass nur der ursprüngliche IBM 4758 Cryptographic Coprocessor auf ihn zugreifen kann.

Bei bestimmten Manipulationsereignissen schützt sich der IBM 4758 Cryptographic Coprocessor selbst, indem der für die Aufnahme von sensiblen Daten vorgesehene Speicher sicher und unwiderruflich komplett gelöscht wird. Zu diesen Daten gehören der Hauptschlüssel, alle beibehaltenen Schlüsseldaten sowie die Informationen über die Zugriffssteuerung. Findet ein Manipulationsereignis statt, das einen solchen Selbstschutz des IBM 4758 Cryptographic Coprocessor durch das komplette Löschen des Speichers auslöst, werden alle beibehaltenen Schlüssel permanent und vollständig zerstört. Falls Sie sich dazu entschlossen haben, den Schlüssel aus einer Komponente in der Hardware beizubehalten, ist die entsprechende Komponente nach einem solchen Ereignis funktionsunfähig.

In einer Installation ohne Beibehaltung ist die Wiederherstellung nach einem Manipulationsereignis unter den folgenden Bedingungen möglich:

- Es wurde zuvor ein Sicherungsklon des IBM 4758 Cryptographic Coprocessor erstellt, der von der Manipulation betroffen war.
- Es wurden zuvor Sicherungen der 'nicht integrierten' verschlüsselten Daten erstellt.

Der Administrator einer durch einen IBM 4758 Cryptographic Coprocessor erweiterten Tivoli PKI-Installation muss die Sicherheitsanforderungen sorgfältig gegen das Erfordernis einer Sicherung und Wiederherstellung von privaten Schlüsseln abwägen. In vielen Fällen kann der Systemaufwand, der mit der Ausstellung eines neuen CA-Zertifikats (und aller von diesem Zertifikat abhängigen Client-Zertifikate) verbunden ist, die Verwendung der Option für die Nicht-Beibehaltung vorgeben.

Im Allgemeinen sollte die Option für die Beibehaltung nur dann verwendet werden, wenn dies eindeutig erforderlich ist und zudem die hiermit verbundenen Nutzen und Risiken grundlegend überdacht wurden. Falls das Tivoli PKI-System in einer Umgebung eingesetzt werden muss, in der durch Standards vorgegeben ist, dass Schlüsselpaare in der Hardware generiert und permanent gespeichert werden müssen, ist die Verwendung der Option für die Beibehaltung erforderlich. In anderen Fällen empfiehlt es sich, diese Option nicht zu verwenden.

Aufgabenbereiche und Profile

Tivoli PKI und der IBM 4758 Cryptographic Coprocessor interagieren über unterschiedliche 4758-Aufgabenbereiche und -Profile, die während der Installation von Tivoli PKI erstellt werden. Die durch Tivoli erstellten Aufgabenbereiche und Profile sind für die Inbetriebnahme und Verwendung eines Systems ausreichend. Bei den meisten Kunden können jedoch hinsichtlich des IBM 4758 Cryptographic Coprocessor zusätzliche Optimierungen und Verwaltungsaktionen erforderlich sein.

Die während des Installationsprozesses von Tivoli PKI erstellten Profile enthalten sowohl für die Profilkennphrase als auch für das Profil selbst Verfallsdaten. Diese Verfallsdaten müssen beachtet werden, und die Profile müssen wie erforderlich geändert und aktualisiert werden. Falls die Gültigkeitsdaten der Profile nicht innerhalb des aktuellen Zeitraums gehalten werden können, kann dies dazu führen, dass Sie aus dem IBM 4758 Cryptographic Coprocessor ’ausgesperrt’ sind.

Als komfortable Sicherheitsfunktion verfügt der IBM 4758 Cryptographic Coprocessor über einen einzigen Aufgabenbereich (DEFAULT), auf den der Zugriff nicht durch eine Kennphrase geschützt ist. Nach der Erstelltung der Tivoli PKI-spezifischen Aufgabenbereiche und Profile wird durch den Installationsprozess ein ’eingeschränktes Standardprofil’ geladen, das die Möglichkeiten dieses nicht geprüften Aufgabenbereichs reduziert. Das ’eingeschränkte’ Standardprofil wurde absichtlich relativ weit gefasst, damit Benutzer, die auf Grund von falschen Kennphrasen oder verfallenen Profilen keinen Zugriff mehr haben, über eine Wiederherstellungsoption verfügen. In fast allen Fällen ist es jedoch sinnvoll, diesen ’eingeschränkten Standardaufgabenbereich’ später über die Installationseinstellungen hinaus zu begrenzen.

Anmerkung: Tivoli empfiehlt dringend die Erstellung eines neuen Aufgabenbereichs, der durch eine sorgfältig gewählte Kennphrase geschützt wird und über ausreichende Zugriffsberechtigungen für eine Wiederherstellung nach Profilsperrungen verfügt.

IBM 4758 Cryptographic Coprocessor in der Tivoli PKI-Umgebung installieren und klonen

Anweisungen zur physischen Installation und zur Softwareinstallation für den IBM 4758 Cryptographic Coprocessor finden Sie in der Dokumentation zum IBM 4758 Cryptographic Coprocessor. Spezifischere Anweisungen enthält die Dokumentation, die Sie im Abschnitt ’Library’ der Webseite zum IBM 4758 Cryptographic Coprocessor unter der folgenden Adresse aufrufen können: http://www.ibm.com/security/cryptocards/.

Physische Installation:

Tivoli PKI 3.7.1 unterstützt nur den ersten IBM 4758 Cryptographic Coprocessor auf jeder physischen Maschine. Wenn sich RA und CA auf derselben Maschine befinden, kann dieser IBM 4758 Cryptographic Coprocessor gemeinsam benutzt werden.

Entsprechende Informationen enthält das *Installationshandbuch zum IBM 4758 Cryptographic Coprocessor*.

Softwareinstallation

Lesen und befolgen Sie alle Anweisungen in der Datei README, die sich im Verzeichnis ’/usr/lpp/csuf’ befindet. Hierbei muss insbesondere darauf geachtet werden, dass die passenden Softwaresegmente für den jeweils installierten spezifischen IBM 4758 Cryptographic Coprocessor geladen werden, damit ein unnötiges erneutes Laden des ersten Segments für den IBM 4758 Cryptographic Coprocessor vermieden werden kann.

Über das Dienstprogramm 'csufclu' können sensible Daten komplett gelöscht werden, indem die Segmente 2 und 3 zurückgesetzt werden. Alternativ kann zu diesem Zweck auch das Dienstprogramm 'csufcnm' verwendet werden. Hierzu werden die Optionen **Crypto Node** > **Initialize** ausgewählt.

Weitere Informationen finden Sie im Handbuch *Version 2.XX CCA Support Program Installation Manual*, Kapitel 3 (Installing the Support Program) und Kapitel 4 (Loading Software into the Coprocessor).

Klonen

Bei den Klonprozeduren, die für den IBM 4758 Cryptographic Coprocessor empfohlen werden, wird lediglich ein gemeinsam benutztes Exemplar des Hauptschlüssels erstellt. Bei einer kompletten Sicherung müssen die Aufgabenbereiche, die Profile und der auf Platte befindliche Speicher, die durch die Einheit verwendet werden, kopiert werden. Sie müssen sicherstellen, dass die Bedingungen für die Übertragung aller installierten Aufgabenbereiche und Profile von der Haupt- an die Sekundäreinheit des IBM 4758 Cryptographic Coprocessor sowie aller Dateien im Verzeichnis '/usr/lpp/csuf/csufkeys' geschaffen werden.

Entsprechende Anweisungen enthält das Handbuch *Version 2.XX CCA Support Program Installation*, Anhang 'Cloning Procedure'.

Empfohlene Dokumentation zum IBM 4758 Cryptographic Coprocessor

Bei der Installation und Konfiguration des IBM 4758 Cryptographic Coprocessor sollten Sie die folgende Produktdokumentation hinzuziehen und sich mit diesen Informationen vertraut machen. Die Angaben in dem vorliegenden Handbuch sind nur als Ergänzung zur Produktdokumentation für den IBM 4758 Cryptographic Coprocessor zu verwenden. Die Produktdokumentation finden Sie unter den folgenden Webadressen:

`http://www.ibm.com/security/cryptocards/`

IBM 4758 Models 002/023 Specification Sheet, (G221-9091-02)
IBM 4758 General Information Manual, (Kapitel 1–3)
IBM 4758 Installation Manual
Version 2.XX CCA Installation Manual,
(Kapitel 1–6 sowie der Anhang 'Master-Key Cloning')
Version 2.XX CCA Basic Services, (Kapitel 1
sowie die Einführungstexte der Kapitel 2 und 3)

Prüfung

Das Tivoli PKI-Prüfsubsystem bietet Unterstützung für die Protokollierung sicherheitsrelevanter Aktionen auf der Grundlage der Empfehlungen des Standards X9.57 für den Finanzsektor. Auf diese Weise können Sie Prüfprotokolle verwalten und archivieren und Integritätsprüfungen von Protokolleinträgen durchführen.

Das Prüfsubsystem besteht aus einer Client-Bibliothek und einem Prüf-Server. Der Prüf-Server empfängt Prüfereignisse von autorisierten Clients und schreibt diese Ereignisse in ein integritätsgeschütztes Prüfprotokoll. Alle Protokolleinträge werden in einer DB2-Datenbank gespeichert. Prüfereignisse werden außerdem in einer Datei gespeichert. Abfrage- und Berichterstellungs-Tools werden von DB2 UDB bereitgestellt.

Protokolleinträge

Protokolleinträge werden in Form eines Prüfprotokolls in einer DB2-Datenbank gespeichert. Das Prüfprotokoll enthält pro Prüfereignis einen Protokolleintrag. Die Prüfdatenbank hilft bei der Manipulationserkennung, wie im Standard für den Finanzsektor X9.57 vorgeschrieben. Jeder Protokolleintrag ist durch eine Seriennummer eindeutig gekennzeichnet.

Prüfereignisse

Tivoli PKI-Prüfereignisse sind Sätze, die die Bedeutung einer sicherheitsrelevanten Task angeben. Der Prüf-Server empfängt Prüfereignisse von autorisierten Clients und schreibt diese Ereignisse in ein integritätsgeschütztes Prüfprotokoll.

Die Tivoli PKI-Prüfereignisse werden in die folgenden Kategorien unterteilt:

- Schlüsselverwaltungsereignisse

  Ereignisse im Zusammenhang mit der sicheren Verwaltung von Schlüsseln, um Benutzern Schlüssel am gewünschten Ort und zur gewünschten Zeit bereitstellen zu können.

- Zertifikatsverwaltungsereignisse

  Ereignisse, die sich aus der Verwaltung digitaler Zertifikate und aus der Pflege von Informationen zu Zertifikaten und CRLs im Directory ergeben.

- Sicherheitsrelevante Ereignisse

  Ereignisse, die sich aus der Ausführung sicherheitsrelevanter Tasks ergeben. Hierzu zählen beispielsweise Integritätsprüfungen, Authentifizierungen und Zertifikatsprüfungen.

- Ereignisse für Prüfadministratoren

  Diese Ereignisse ergeben sich aus Aktionen, die mit den Aufgaben von Prüfadministratoren zusammenhängen. Die Aufgaben eines Prüfadministrators umfassen die Implementierung der Sicherheitsregeln Ihres Unternehmens.

- RA-Ereignisse

  Ereignisse, die sich aus den Aktionen einer RA ergeben.

Nähere Informationen zu Prüfereignissen finden Sie im Abschnitt „Felder für Prüfereignisse” auf Seite 125.

Masken für Prüfereignisse

In Tivoli PKI bieten Masken für Prüfereignisse Unterstützung für die Steuerung der Prüfereignisse, die an den Prüf-Server weitergeleitet werden. Beachten Sie, dass eine verbindliche Untermenge von Prüfereignissen nicht von Maskenspezifikationen beeinflusst wird.

Informationen zum Definieren einer Maske für Prüfereignisse finden Sie im Abschnitt „Prüfmaske definieren” auf Seite 49.

Verbindliche und optionale Prüfereignisse

Eine bestimmte Untermenge von Prüfereignissen ist verbindlich. Diese Ereignisse werden von Maskendefinitionen in der Konfigurationsdatei des Prüf-Clients nicht betroffen. Informationen zu verbindlichen und optionalen Prüfereignissen finden Sie in Tabelle 19 auf Seite 126.

Integritätsprüfung

Tivoli PKI bietet ein Tool, mit dem geprüft werden kann, ob Prüfsätze unberechtigterweise verändert wurden. Dieses Tool trägt die Bezeichnung Audit Integrity Check. Integritätsprüfungen unterscheiden sich von Maßnahmen zum Schutz der Vertraulichkeit von Daten zum Zwecke der Geheimhaltung.

Der Prüf-Server unterzeichnet nicht jeden Eintrag. Statt dessen wendet er auf jeden Eintrag einen Nachrichtenauthentifizierungscode (MAC = Message Authentication Code) an und verwaltet einen MAC für die gesamte Datenbank.

Integritätsversiegelung

In Tivoli PKI bedeutet Integritätsversiegelung das Unterzeichnen archivierter Datenbankdateien mit Prüfprotokollen. Das Unterzeichnen erfolgt mit Hilfe des Tivoli PKI-Befehlszeilen-Tools 'Audit Archive and Sign'.

Prüfprotokoll archivieren

Tivoli PKI unterstützt das Archivieren des aktuellen Prüfprotokolls in eine Archivdatei. Hierzu wird das Befehlszeilen-Tool 'Audit Archive and Sign' verwendet.

DB2 Datenbanken

IBM DB2 Universal Database (DB2 UDB) ist ein web-fähiges Verwaltungssystem für relationale Datenbanken mit Java-Unterstützung. In Tivoli PKI können mit IBM DB2 Universal Database folgende Tasks ausgeführt werden:

- Verwalten von Informationen zu Registrierungsprozessen für digitale Zertifikate.
- Speichern von Informationen zu RA-Aktionen, mit denen Anforderungen für digitale Zertifikate genehmigt oder zurückgewiesen werden. Diese Informationen werden zu Prüfungszwecken verwendet.
- Bereitstellen von Betriebsstatistiken zur Gesamtauslastung der Tivoli PKI-Registrierungseinrichtung.
- Bereitstellen von Datenbanken für den Tivoli PKI-CA, die RA, das Prüfsubsystem, das Directory, die Funktion zum Sichern und Wiederherstellen von Schlüsseln und die Tivoli PKI-Konfigurationsdaten.

Webserver

Web-Server sind Server-Programme, die auf Informationsanforderungen von Browsern reagieren. Tivoli PKI verwendet IBM WebSphere-Softwareprodukte, um eine gesicherte Grundlage für solche Netztransaktionen bereitzustellen. Der WebSphere Application Server und der IBM HTTP Server stellen in Tivoli PKI die Infrastruktur für Web-Server-Funktionalität zur Verfügung.

In einem Tivoli PKI-System befindet sich die Web-Server-Software auf der gleichen Maschine wie die RA. Sie ermöglicht eine sichere Abgrenzung zwischen geschützten Programmen und den Benutzern, die auf diese Programme zugreifen wollen. Mit Hilfe der HTTP- und HTTPS- (Hypertext Transfer Protocols) sowie der SSL-Technologie (Secure Sockets Layer) kann das Web-Server-Produkt die Kommunikation zwischen Client und Server verschlüsseln. Darüber hinaus können Client-Authentifizierungen durchgeführt werden, um unbefugten Zugriff oder Datenmanipulationen zu verhindern.

IBM WebSphere Application Server

Der IBM WebSphere Application Server (WAS) ist ein Server für Java-Anwendungen, der die Verwaltung und Nutzung von Web-Anwendungen vereinfachen soll. WAS muss auf einem Host-Web-Server installiert sein, der HTTP-Anforderungen von Browsern verarbeitet und die Antworten über das HTTP-Protokoll im HTML-Format zurückgibt.

Bei der Installation von WebSphere wird die Konfiguration des entsprechenden Host-Webservers so verändert, dass bestimmte Anforderungen zur Verarbeitung an WebSphere und nicht an den Webserver weitergeleitet werden. WAS nutzt eine Java-Entwicklungs- und -Laufzeitumgebung auf der Host-Maschine. Diese Java-Umgebung ermöglicht WebSphere die Ausführung von Java-Programmen, die von der Tivoli PKI-Registrierungseinrichtung verwendet werden.

IBM HTTP Server

Der Tivoli PKI-Server basiert auf einem Modell mit drei Servern und drei Ports, um die Client-Anforderungen zu verarbeiten. Ihr Unternehmen hat sich möglicherweise für die Installation eines einzigen Exemplars des IBM HTTP Server und für die Konfiguration verschiedener virtueller Host-Namen und Ports entschieden, um verschiedene Arten von Anforderungen verarbeiten zu können.

Mit diesem Modell verarbeitet Tivoli PKI folgende Arten von Anforderungen:

- Anforderungen, die keine Verschlüsselung oder Authentifizierung benötigen.
- Anforderungen, die Verschlüsselung und Server-Authentifizierung benötigen.
- Anforderungen, die Verschlüsselung sowie Server- und Client-Authentifizierung benötigen.

Tabelle 11 fasst diese Konfigurationsalternativen zusammen.

Tabelle 11. Modell für IBM HTTP Server mit drei Servern und drei Ports

Protokoll	SSL	Server-Authentifizierung	Client-Authentifizierung	Beispiel für Port-Nummer bei einer IP	Beispiel für Port-Nummer bei mehreren IPs
HTTP	Nein	Nein	Nein	80	80
HTTPS	Ja	Ja	Nein	443	443
HTTPS	Ja	Ja	Ja	1443	443

IP-Aliasing

Im Bereich der Internet-Technologie ist ein Aliasname ein Name, der einem Server zugeordnet wird, so dass der Server vom Namen seiner Host-Maschine unabhängig wird. Der Aliasname muss im Domain Name System (DNS) Ihres Systems definiert werden.

Directory-Server

Tivoli PKI verwendet das IBM SecureWay Directory zur Speicherung von digitalen X.509-Zertifikaten, Zertifikatswiderrufslisten (CRLs), CA-Regeln und weiteren Informationen zu registrierten Servern und Benutzern. Mit dieser Komponente kann nach einem Zertifikat für einen öffentlichen Schlüssel einer bestimmten Person oder eines Servers gesucht werden. Hierzu wird das Directory nach dem eindeutigen registrierten Namen (DN) der Person oder des Servers oder nach anderen relevanten Informationsquellen durchsucht.

Dieser Server unterstützt LDAP-Standards (LDAP = Lightweight Directory Access Protocol) und basiert auf DB2 UDB. Er wird als eigenständiger Dämon ausgeführt und verwendet ein Client/Server-Modell, um Tivoli PKI den Zugriff auf den Server zu ermöglichen. Der Server nutzt eine Schnittstelle auf Web-Basis, um das Directory einzurichten, zu verwalten und die enthaltenen Daten anzuzeigen. Als Directory kann ein vorhandener Server oder ein speziell für Tivoli PKI installierter und konfigurierter Server dienen.

Objektkennungen

Eine Objektkennung (OID = Object Identifier) ist ein Wert, der sich von allen ähnlichen Werten unterscheidet und der einem Objekt zugeordnet ist. Jede gemäß ASN.1 definierte OID bildet einen Knoten einer Baumstruktur (ähnlich wie bei DIT). Eine Objektkennungsbaumstruktur ist eine Baumstruktur, deren Stamm den ITU-Empfehlungen X.680 entspricht. Die Scheitelpunkte entsprechen Administratorberechtigungen für die Zuordnung von Bögen (Segmenten, die zwei Scheitelpunkte verbinden) von diesem Scheitelpunkt (ein Punkt, der sich am Ende eines Bogens oder am Schnittpunkt von Bögen befinden kann).

Jeder Bogen in der Baumstruktur ist durch eine Objektkennungskomponente (ein numerischer Wert) gekennzeichnet. Jedes zu unterzeichnende Objekt ist genau einem Scheitelpunkt (in der Regel ein Blatt des Baums) zugeordnet. Kein anderes Objekt (der gleichen oder einer anderen Art) wird diesem Scheitelpunkt zugeordnet. Aus diesem Grund wird ein Objekt eindeutig durch die Reihenfolge der numerischen Werte (Objektkennungskomponenten) der Bögen vom Stamm bis zum Scheitelpunkt des Objekts unterzeichnet.

Direkt unterhalb des Stamms werden derzeit drei Werte definiert. Sie lauten 0, 1 und 2:

- 0 wird CCITT-Empfehlungen zugewiesen.
- 1 wird ISO-Empfehlungen zugewiesen.
- 2 wird beiden Unternehmen gemeinsam zugewiesen.

So fallen beispielsweise alle OIDs, die für den Directory-Standard definiert sind, unter die gemeinsame CCITT/ISO-Kategorie 2 und werden der Objektkennungskomponente 5 zugeordnet. Aus diesem Grund beginnen alle OIDs für Directory-Standardobjekte mit dem Präfix 2.5.

5

Referenzinformationen

Dieses Kapitel enthält Referenzinformationen zu folgenden Themen:

- Konfigurationsdateien

  Informationen zu Parameternamen, Beschreibungen und Formaten. Es wird angegeben, ob die Parameter verbindlich oder optional sind und ob sie konfiguriert werden können.

- Befehle

  Syntax- und Parameterbeschreibungen für die Tivoli PKI-Befehlszeilendienstprogramme.

- Felder für Prüfereignisse

  Dieser Abschnitt erläutert die Informationen, die in Tivoli PKI-Prüfereignissen enthalten sind.

- Prüfereignisse

  Dieser Abschnitt erläutert Prüfereignisse und gibt an, ob ein Ereignis verbindlich oder optional ist.

- Daten der Prüfdatenbank

  Dieser Abschnitt beschreibt die Speicherung von Protokolleinträgen in den Tabellen der relationalen Datenbank. Hier finden Sie Informationen zu den Feldnamen im Datensatz (bzw. den Spaltennamen in der Tabelle), zu den Speicherorten der Daten sowie Beschreibungen der Felder und der Datenformate.

- Fehlerbehebung

  Dieser Abschnitt enthält Informationen zur grundlegenden Fehlerbehebung sowie zur Nachrichtenerstellung auf Debug-Stufe.

Konfigurationsdateien

Dieser Abschnitt enthält die Beschreibungen der Parameter für folgende Konfigurationsdateien:

- Konfigurationsdatei ’jonahca.ini’ für CA-Server
- Konfigurationsdatei ’jonahra.ini’ für RA-Server
- Konfigurationsdatei ’AuditServer.ini’ für Prüfserver
- Konfigurationsdatei ’AuditClient.ini’ für Prüf-Client

Tabelle 12. Tivoli PKI-Konfigurationsdateien

AIX-Standardpfad	Windows NT-Standardpfad	Beschreibung
/usr/lpp/iau/etc/TrustAuthority/ jonahca.ini	c:\Program Files\IBM\Trust Authority\etc\TrustAuthority\jonahca.ini	Die Konfigurationsdatei des CA-Servers. Diese Datei enthält die Konfigurationsvariablen des CA-Servers. Sie können diese Variablen ändern, um grundlegende Funktionsmerkmale und Verbindungseinstellungen festzulegen.
/usr/lpp/iau/pkrf/Domains/ YourDomain/etc/jonahra.ini	c:\Program Files\IBM\Trust Authority \pkrf\Domains\YourDomain\etc\ jonahra.ini	Die Konfigurationsdatei des RA-Servers. Diese Datei enthält die Konfigurationsvariablen des RA-Servers. Neben den grundlegenden Funktionsmerkmalen und Verbindungseinstellungen ermöglichen diese Variablen die Steuerung der Interaktion von RA- und Directory-Server.
/usr/lpp/iau/etc/AuditClient.ini	c:\Program Files\IBM\Trust Authority\etc\AuditClient.ini	Die Konfigurationsdatei des Prüf-Clients. Diese Datei enthält die Konfigurationsvariablen der Prüf-Clients. Die Variablen ermöglichen Verbindungseinstellungen und unterstützen die Optimierung der Prüfmaske, die die Weiterleitung von Prüfereignissen steuert.
/usr/lpp/iau/etc/TrustAuthority/AuditServer.ini	c:\Program Files\IBM\Trust Authority\etc\TrustAuthority\ AuditServer.ini	Die Konfigurationsdatei des Prüf-Servers. Diese Datei enthält die Konfigurationsvariablen des Prüf-Servers. Sie können diese Variablen ändern, um grundlegende Funktionsmerkmale und Verbindungseinstellungen des Prüf-Servers neu zu konfigurieren und um das Protokollieren von Debug- und Fehlernachrichten zu steuern. Die Variablen legen außerdem fest, welche Ereignisse protokolliert werden.

Dateibeschreibung

Eine Konfigurationsdatei ist in Abschnitte unterteilt. Jeder Abschnitt beginnt mit einer Kopfzeile, die in eckigen Klammern eingeschlossen ist. Beispiel: *[Abschnitt]*. Ein Abschnitt kann eine oder mehrere Anweisungen mit Zuordnungen von Parametern und Werten (*Parameter=Wert*) enthalten.

Die hier aufgeführten Tabellen enthalten alle Abschnitte und Parameter der Tivoli PKI-Konfigurationsdateien, die zum Zwecke der Systemverwaltung editiert werden können.

Die Tabellen enthalten folgende Spalten:

- **Parameter**
- **Beschreibung**
- **Wert gemäß Standardkonfiguration**

  Diese Spalte enthält den Standardwert, sofern vorhanden. Wenn ein Standardwert existiert, ist ein Parameter optional, andernfalls ist er erforderlich.
- **Nach Konfiguration problemlos änderbar?**

  Diese Spalte gibt darüber Aufschluss, ob der angegebene Wert geändert werden kann.

Dieses System ignoriert Leerzeichen. Einheiten müssen in der korrekten Reihenfolge eingegeben werden.

Konfigurationsdatei für CA-Server

Tabelle 13 auf Seite 86 enthält eine Beschreibung der Parameter der Konfigurationsdatei für CA-Server, jonahca.ini.

Tabelle 13. CA-Server - Konfigurationsdatei

Parameter	Beschreibung	Wert gemäß Standardkonfiguration	Nach Konfiguration problemlos änderbar?
[OIDs] Standardmechanismus zur eindeutigen Identifizierung von Elementen			
C=	OID für Land	2.5.4.6	Nein
O=	OID für Unternehmen	2.5.4.10	Nein
OU=	OID für Unternehmen	2.5.4.11	Nein
CN=	OID für allgemeinen Namen	2.5.4.3	Nein
L=	OID für Ort	2.5.4.7	Nein
ST=	OID für Bundesland	2.5.4.8	Nein
T=	OID für Titel	2.5.4.12	Nein
DC=	OID für Domänenkomponente	0.9.2342.19200300.100.1.25	Nein
id-dsa=	OID für DSA	1.2.840.10040.4.1	Nein
id-dsa-with-sha1=	OID für DSA mit SHA-1	1.2.840.10040.4.3	Nein
rsaEncryption=	OID für RSA-Verschlüsselung	1.2.840.113549.1.1.1	Nein
sha-1WithRSAEncryption=	OID für SHA-1 mit RSA-Verschlüsselung	1.2.840.113549.1.1.5	Nein
sha1=	OID für SHA-1	1.3.14.3.2.26	Nein
hmac-sha1=	OID für SHA-1- Hash-Nachrichtenauthentifizierungscode	1.3.6.1.5.5.8.1.2	Nein
pkcs7-data=	OID für PKCS#7	1.2.840.113549.1.7.1	Nein
pkcs12-certbag=	OID für Zertifikattasche	1.2.840.113549.1.12.10.1.3	Nein
pkcs12-keybag=	OID für Schlüsseltasche	1.2.840.113549.1.12.10.1.1	Nein
X509-Certificate=	OID für X.509-Zertifikat	1.2.840.113549.1.9.22.1	Nein
PasswordBasedMAC=	OID für MAC auf Kennwortbasis	1.2.840.113533.7.66.13	Nein
MyPolicy=	Beispiel für die Eingabe einer OID für PolicyName1 im Abschnitt CertPolicy	1.34.67.7	Nein
My Lite Policy=	Beispiel für die Eingabe einer OID für PolicyName2 im Abschnitt CertPolicy	2.4.1.0	Nein
[AsymmetricKeyAlgs]			

Tabelle 13. CA-Server - Konfigurationsdatei (Forts.)

Parameter	Beschreibung	Wert gemäß Standardkonfiguration	Nach Konfiguration problemlos änderbar?
DSA=	Definition des DSA-Schlüsselalgorithmus	id-dsa	Nein
RSA=	Definition des RSA-Schlüsselalgorithmus	rsaEncryption	Nein
[AsymmetricEncAlgs]			
DSA=	Definition des DSA-Verschlüsselungsalgorithmus	id-dsa	Nein
[AsymmetricSigAlgs]			
DSAwithSHA1=	Definition des DSA mit SHA-1-Unterschriftsalgorithmus. Wird von der GUI oder dem Server zur Anzeige und zur Auswahl des Algorithmus verwendet.	id-dsa-with-sha1	Nein
RSAwithSHA1=	Definition des RSA mit SHA-1-Unterschriftsalgorithmus. Wird von der GUI oder dem Server zur Anzeige und zur Auswahl des Algorithmus verwendet.	sha-1WithRSAEncryption	Nein
RSAwithMD5=	Definition des RSA mit MD5-Unterschriftsalgorithmus. Wird von der GUI oder dem Server zur Anzeige und zur Auswahl des Algorithmus verwendet.		
[ObjectStore]			
Name=	Dateistamm (ohne Erweiterung) zur Verwendung mit CA-Datendateien	caObjectStore	Nein
Path=	Absoluter Pfad für Tivoli PKI-CA-Dateien	Für Windows NT: c:\Program Files\IBM\Trust Authority\etc\TrustAuthority\ Für AIX: /usr/lpp/iau/etc/TrustAuthority/	Nein

Tabelle 13. CA-Server - Konfigurationsdatei (Forts.)

Parameter	Beschreibung	Wert gemäß Standardkonfiguration	Nach Konfiguration problemlos änderbar?
[CertPolicy] Für jeden Unterschriftsalgorithmus muss im OID-Abschnitt eine OID deklariert werden. Für jeden Regelnamen muss im OID-Abschnitt eine entsprechende OID vorhanden sein.			
SigAlg1=	Definition des ersten Unterschriftsalgorithmus. Ein entsprechender Eintrag im OID-Abschnitt ist erforderlich.	sha-1WithRSAEncryption	Nein
StartTimeSpecifiable=	Gibt an, ob der Anfordernde (Client-Entität an RA oder RA an CA) die Startzeit angeben kann.	T	Nein
MaxLifetime=	Die maximale Gültigkeitsdauer eines Zertifikats (in Stunden).	17544h	Ja
LifeTimeDef=	Die standardmäßige Gültigkeitsdauer eines Zertifikats (in Tagen).	180d	Nein
KeySpecifiable=	Gibt an, ob der Anfordernde (Client-Entität oder RA) den allgemeinen Schlüssel des Zertifikatsgegenstands angeben kann.	T	Nein
KeyUsageSupported=	Gibt an, ob die Erweiterung der Schlüsselverwendung unterstützt wird.	T	Nein
KeyUsageRequired=	Gibt an, ob die Erweiterung der Schlüsselverwendung erforderlich ist.	F	Nein
PolicyCritical=	Gibt an, ob es sich um eine kritische Regel handelt.	F	Nein
PolicyRequired=	Gibt an, ob die Regel erforderlich ist.	F	Nein
PolicyName1=	Der Name der primären Regel. Hierfür muss im OID-Abschnitt eine entsprechende OID vorliegen.	MyPolicy	Nein
Policy1Org=	Der Name des Unternehmens, das diese Regel benötigt.	Ihr Unternehmen	Nein
Policy1Notice1=	Notice1 wird Policy1 zugeordnet	3	Nein
Policy1Notice2=	Notice2 wird Policy1 zugeordnet	17	Nein

Tabelle 13. CA-Server - Konfigurationsdatei (Forts.)

Parameter	Beschreibung	Wert gemäß Standardkonfiguration	Nach Konfiguration problemlos änderbar?
UserNoticeText1=	Ein juristischer Hinweis oder eine Ablehnungserklärung, die die andere Partei lesen und bei Entscheidungen berücksichtigen muss.	Juristischer Hinweis oder Ablehnungserklärung	Nein
CPS1=	URL-Adresse, unter der die Anweisung für Policy1 verfügbar ist.	http://localhost/index.html	Nein
PolicyName2=	Name der sekundären Regel. Ist dieser Name vorhanden, muss eine entsprechende OID im OID-Abschnitt angegeben werden.	My Lite Policy	Nein
CPS2=	URL-Adresse, unter der die Anweisung für Policy2 verfügbar ist.	http://localhost/index.html	Nein
TimeBetweenCRLs=	Standardzeit zwischen geplanten CRL-Publizierungen	1d	Ja
CRLDuration=	CRL-Gültigkeitsdauer	2d	Ja
[CrossCertPolicy]			
SigAlg1=	Definition des ersten Unterschriftsalgorithmus. Ein entsprechender Eintrag im OID-Abschnitt ist erforderlich.	sha-1WithRSAEncryption	Nein
StartTimeSpecifiable=	Gibt an, ob der Anfordernde (Client-Entität oder RA) die Startzeit angeben kann.	T	Nein
MaxLifeTime	Die maximale Gültigkeitsdauer eines Zertifikats.	17544h	Ja
LifeTimeDef	Die Standardgültigkeitsdauer eines Zertifikats.	180d	Nein

Tabelle 13. CA-Server - Konfigurationsdatei (Forts.)

Parameter	Beschreibung	Wert gemäß Standardkonfiguration	Nach Konfiguration problemlos änderbar?
KeySpecifiable=	Gibt an, ob der Anfordernde (Client-Entität oder RA) den allgemeinen Schlüssel des Zertifikatsgegenstands angeben kann.	T	Nein
KeyUsageSupported=	Gibt an, ob die Erweiterung der Schlüsselverwendung unterstützt wird.	T	Nein
KeyUsageRequired=	Gibt an, ob die Erweiterung der Schlüsselverwendung erforderlich ist.	F	Nein
PolicyCritical=	Gibt an, ob es sich um eine kritische Regel handelt.	F	Nein
PolicyRequired=	Gibt an, ob die Regel erforderlich ist.	F	Nein
PolicyName1=	Der Name der primären Regel. Hierfür muss im OID-Abschnitt eine entsprechende OID vorliegen.	MyPolicy	Nein
Policy1Org=	Der Name des Unternehmens, das diese Regel benötigt.	Ihr Unternehmen	Nein
Policy1Notice1=	Notice1 wird Policy1 zugeordnet	3	Nein
Policy1Notice2=	Notice2 wird Policy1 zugeordnet	17	Nein
UserNoticeText1=	Ein juristischer Hinweis oder eine Ablehnungserklärung, die die andere Partei lesen und bei Entscheidungen berücksichtigen muss.	Juristischer Hinweis oder Ablehnungserklärung	Nein
CPS1=	URL-Adresse, unter der die Anweisung für Policy1 verfügbar ist.	http://localhost/index.html	Nein
PolicyName2=	Name der sekundären Regel.	My Lite Policy	Nein
CPS2=	URL-Adresse, unter der die Anweisung für Policy2 verfügbar ist.	http://localhost/index.html	Nein
TimeBetweenCRLs=	Standardzeit zwischen geplanten CRL-Publizierungen	1d	Ja
CRLDuration=	CRL-Gültigkeitsdauer	2d	Ja

Tabelle 13. CA-Server - Konfigurationsdatei (Forts.)

Parameter	Beschreibung	Wert gemäß Standardkonfiguration	Nach Konfiguration problemlos änderbar?
[General]			
MyName=	DN der Client-Entität.	/C=US/O=Ihr Unternehmen/OU=Trust Authority/CN=Trust Authority CA	Nein
DefaultRA=	Die Standard-RA	1	Nein
PreferredCryptoProvider=	Die GUID (Globally Unique Identifier) des Verschlüsselungsanbieters.	dda0c1e0-7b73-11d0-8e0c-0004ac602b18	Nein
CertperDP=	Zertifikate pro Verteilungspunkt	0	Ja
CRLDistName=	Name des in das Zertifikat einzutragenden Verteilungspunkts.	MyCRLDistName%d	Ja
TempPath=	Pfad zur Speicherung temporärer Dateien.	Für Windows NT: c:\Program Files\IBM\Trust Authority\etc\TrustAuthority\ Für AIX: /usr/lpp/iau/etc/TrustAuthority/	Nein
PathToDLLs=	Pfad zur Speicherung von PKIX-Bibliotheken.	Für Windows NT: c:\pkix\ Für AIX: /usr/pkix/	Nein
RA1=	DN der RA für diesen CA.	/C=US/O=Ihr Unternehmen/OU=Trust Authority/CN=Trust Authority RA	Nein
[Transport]			
TCPPort=	TCP-Port, der vom CA überwacht wird.	1830	Ja
TCPHost=	Host-Name der Maschine, auf der sich der CA befindet.	*Ihr Host-Name*	Nein
PollInterval=	Sendeaufrufintervall.	10s	Ja
RetryInterval=	Wiederholungsintervall	10m	Ja
[KeyStore]			
CurKeyStore=	Momentan verwendeter KeyStore	VSC	Nein

Tabelle 13. CA-Server - Konfigurationsdatei (Forts.)

Parameter	Beschreibung	Wert gemäß Standardkonfiguration	Nach Konfiguration problemlos änderbar?
[VSC] Dieser Abschnitt ist erforderlich, wenn der Wert des Parameters 'CurKeyStore' 'VSC' lautet.			
Model=	Art des verwendeten Speichers.	PKCS11_STORAGE_MODEL	Nein
Guid=	Global Unique Identifier.	7F529C80-C942-11D1-8FB0-0004AC61389A	Nein
InitialSOpw=	Anfangskennwort für den Prüfadministrator.	SOPIN	Nein
TokenDir=	Absoluter Pfad und Dateiname für die virtuelle Smart Card.	Für Windows NT: c:\Program Files\IBM\Trust Authority\etc\TrustAuthority\caKS.fil Für AIX: /usr/lpp/iau/etc/TrustAuthority/caKS.fil	Nein
4758GUID=	GUID für Einheit IBM 4758.	474d0880-b44c-11d1-b1cf-002035680b00	Nein
Use4758=	Gibt an, ob der CA die Einheit IBM 4758 nutzt.	false	Nein
4758ProfileUserid=	Die Benutzer-ID des 4758-Profils. Nur verfügbar bei Einstellung Use4758=true.	IBMCA001	Nein
4758ProfilePassPhrase=	Das Kennwort des 4758-Profils. Nur verfügbar bei Einstellung Use4758=true.	Secure99	Nein
4758Retain=	Gibt an, ob der CA die Option 4758Retain nutzt. Nur verfügbar bei Einstellung Use4758=true.	false (true nur bei Option RETAIN, die jedoch nicht empfohlen wird)	Nein
4758KeyLength=	Die Länge des 4758-Schlüssels. Mögliche Werte sind: 512,1024 und 2048. Nur verfügbar bei Einstellung Use4758=true.	512	Nein
[TrustPolicy]			
UseCRLs=	Gibt an, ob CRLs und ARLs als Teil des Prüfprozesses verwendet werden sollen.	T	Nein
AllowExpiredCRLs=	Gibt an, ob abgelaufene CRLs zulässig sind.	F	Nein

Tabelle 13. CA-Server - Konfigurationsdatei (Forts.)

Parameter	Beschreibung	Wert gemäß Standardkonfiguration	Nach Konfiguration problemlos änderbar?
AllowFutureCRLs=	Gibt an, ob CRLs mit zukünftigen Datumsangaben zulässig sind.	F	Nein
AllowExpiredCertificates=	Gibt an, ob abgelaufene Zertifikate zulässig sind.	F	Nein
AllowFutureCertificates=	Gibt an, ob Zertifikate mit zukünftigen Datumsangaben zulässig sind.	F	Nein
AllowCRLSearchToFail=	Gibt an, ob ein Fehler vorliegt, wenn keine CRLs oder ARLs für einen Aussteller gefunden werden.	F	Nein
MaximumChainSearchDepth=	Maximale Verkettungstiefe bei rekursiven breitenorientierten Verkettungen	15	Nein
[RemoteServer]			
MaxSessions=	Optimierungsparameter.	16	Nein
EncryptionPolicy=	Gibt an, ob für die Verbindung zwischen einem Hintergrund-Server und dessen fernem Administrator eine Verschlüsselungsregel angewendet wird, wenn sich beide auf dem selben System befinden.	F	Nein
NumAdmins=	Anzahl der zertifizierten Administratoren.	0	Nein
Admin1DN=	DN von Administrator1.	Nicht verwendet	Nein
[ICL]			
IclOdbcProvider=	Art des Anbieters für ODBC.	UDB	Nein

Tabelle 13. CA-Server - Konfigurationsdatei (Forts.)

Parameter	Beschreibung	Wert gemäß Standardkonfiguration	Nach Konfiguration problemlos änderbar?
IclProtectionPolicy	ICL-Schutzregel. Werte: Ignore ContinueWithMessage TerminateTransaction	ContinueWithMessage	Ja
IclOdbcDriverConnect=	Name der Datenbank für ICL.	DSN=ibmdb	Nein
MACLabel=	Kennsatz für MAC-Schlüssel in KeyStore.	CA_MAC_Key	Nein
[URLs]			
/C%EQ%US/O%EQ%Ihr Unternehmen/OU%EQ%Trust Authority/CN%EQ%Trust Authority RA=pkix://localhost:829	Dieser Eintrag wird bei der Konfiguration mit der URL-Adresse und dem DN für die RA gesetzt.	RA DN	Ja

Konfigurationsdatei für RA-Server

Tabelle 14 auf Seite 96 enthält Informationen zu den Parametern der RA-Server-Konfigurationsdatei ’jonahra.ini’.

Tabelle 14. RA-Server - Konfigurationsdatei

Parameter	Beschreibung	Wert gemäß Standardkonfiguration	Nach Konfiguration problemlos änderbar?
[OIDs]			
C=	OID für Land	2.5.4.6	Nein
O=	OID für Unternehmen	2.5.4.10	Nein
OU=	OID für Organisationseinheit	2.5.4.11	Nein
CN=	OID für allgemeinen Namen	2.5.4.3	Nein
L=	OID für Ort	2.5.4.7	Nein
ST=	OID für Bundesland	2.5.4.8	Nein
T=	OID für Titel	2.5.4.12	Nein
DC=	OID für Domänenkomponente	0.9.2342.19200300.100.1.25	Nein
id-dsa=	OID für DSA	1.2.840.10040.4.1	Nein
id-dsa-with-sha1=	OID für DSA mit SHA-1	1.2.840.10040.4.3	Nein
rsaEncryption=	OID für RSA-Verschlüsselung	1.2.840.113549.1.1.1	Nein
sha-1WithRSAEncryption=	OID für SHA-1 mit RSA-Verschlüsselung	1.2.840.113549.1.1.5	Nein
sha1=	OID für SHA-1	1.3.14.3.2.26	Nein
hmac-sha1=	OID für SHA-1- Hash-Nachrichtenauthentifizierungscode	1.3.6.1.5.5.8.1.2	Nein
pkcs7-data=	OID für PKCS#7	1.2.840.113549.1.7.1	Nein
pkcs12-certbag=	OID für PKCS#12-Zertifikatstasche	1.2.840.113549.1.12.10.1.3	Nein
pkcs12-keybag=	OID für PKCS#12-Schlüsseltasche	1.2.840.113549.1.12.10.1.1	Nein
X509-Certificate=	OID für X.509-Zertifikat	1.2.840.113549.1.9.22.1	Nein
PasswordBasedMAC=	OID für MAC auf Kennwortbasis.	1.2.840.113533.7.66.13	Nein
MyPolicy=	Beispiel für die Eingabe einer OID für PolicyName1 im Abschnitt CertPolicy	1.34.67.7	Nein
My Lite Policy=	Beispiel für die Eingabe einer OID für PolicyName2 im Abschnitt CertPolicy	2.4.1.0	Nein

Tabelle 14. RA-Server - Konfigurationsdatei (Forts.)

Parameter	Beschreibung	Wert gemäß Standardkonfiguration	Nach Konfiguration problemlos änderbar?
[AsymmetricKeyAlgs]			
DSA=	Definition des DSA-Schlüsselalgorithmus	id-dsa	Nein
RSA=	Definition des RSA-Algorithmus	rsaEncryption	Nein
[AsymmetricEncAlgs]			
DSA=	Definition des DSA-Verschlüsselungsalgorithmus	id-dsa	Nein
[AsymmetricSigAlgs]			
DSAwithSHA1=	Definition des DSA mit SHA-1-Unterschriftsalgorithmus. Wird von der GUI oder dem Server zur Anzeige und zur Auswahl des Algorithmus verwendet.	id-dsa-with-sha1	Nein
RSAwithSHA1=	Definition des RSA mit SHA-1-Unterschriftsalgorithmus. Wird von der GUI oder dem Server zur Anzeige und zur Auswahl des Algorithmus verwendet.	sha-1WithRSAEncryption	Nein
RSAwithMD5=	Definition des RSA mit MD5-Unterschriftsalgorithmus. Wird von der GUI oder dem Server zur Anzeige und zur Auswahl des Algorithmus verwendet.		
[ObjectStore]			
Name=	Dateiname ohne Erweiterung für RA-Datendateien.	raObjectStore	Nein
Path=	Absoluter Pfad für Tivoli PKI-RA-Dateien	Für Windows NT: c:\Program Files\IBM\Trust Authority\pkrf\Domains\YourDomain\etc\ Für AIX: /usr/lpp/iau/pkrf/Domains/YourDomain/etc/	Nein

Tabelle 14. RA-Server - Konfigurationsdatei (Forts.)

Parameter	Beschreibung	Wert gemäß Standardkonfiguration	Nach Konfiguration problemlos änderbar?
[IssuerCertPolicy] Für jeden Unterschriftsalgorithmus muss im OID-Abschnitt eine OID deklariert werden. Für jeden Regelnamen muss im OID-Abschnitt eine entsprechende OID vorhanden sein.			
SigAlg1=	Definition des Unterschriftsalgorithmus. Ein entsprechender Eintrag im OID-Abschnitt ist erforderlich.	sha-1WithRSAEncryption	Nein
StartTimeSpecifiable=	Gibt an, ob der Anfordernde (Client-Entität an RA oder RA an CA) die Startzeit angeben kann.	T	Nein
MaxLifeTime=	Die maximale Gültigkeitsdauer eines Zertifikats.	8760h	Nein
LifeTimeDef=	Die standardmäßige Gültigkeitsdauer eines Zertifikats.	180d	Nein
KeySpecifiable=	Gibt an, ob der Anfordernde (Client-Entität oder RA) den allgemeinen Schlüssel des Zertifikatsgegenstands angeben kann.	T	Nein
KeyUsageSupported=	Gibt an, ob die Erweiterung der Schlüsselverwendung unterstützt wird.	T	Nein
KeyUsageRequired=	Gibt an, ob die Erweiterung der Schlüsselverwendung erforderlich ist.	F	Nein
PolicyCritical=	Gibt an, ob es sich um eine kritische Regel handelt.	F	Nein
PolicyRequired=	Gibt an, ob die Regel erforderlich ist.	F	Nein
PolicyName1=	Der Name der primären Regel. Hierfür muss im OID-Abschnitt eine entsprechende OID vorliegen.	MyPolicy	Nein
Policy1Org=	Der Name des Unternehmens, das diese primäre Regel benötigt.	Ihr Unternehmen	Nein

Tabelle 14. RA-Server - Konfigurationsdatei (Forts.)

Parameter	Beschreibung	Wert gemäß Standardkonfiguration	Nach Konfiguration problemlos änderbar?
Policy1Notice1=	Notice1 wird Policy1 zugeordnet.	3	Nein
Policy1Notice2=	Notice2 wird Policy2 zugeordnet.	17	Nein
UserNoticeText1=	Ein juristischer Hinweis oder eine Ablehnungserklärung, die die andere Partei lesen und bei Entscheidungen berücksichtigen muss.	Juristischer Hinweis oder Ablehnungserklärung	Nein
CPS1	URL-Adresse, unter der die Anweisung für Policy1 verfügbar ist.	http://localhost/index.html	Nein
PolicyName2=	Name der sekundären Regel. Ist dieser Name vorhanden, muss eine entsprechende OID im OID-Abschnitt angegeben werden.	My Lite Policy	Nein
CPS2=	URL-Adresse, unter der die Anweisung für Policy2 verfügbar ist.	http://localhost/index.html	Nein
EERevokeRequests=	Gibt an, ob eine Client-Entität den Widerruf eines Zertifikats anfordern kann. Lautet der Wert 'ANY', kann die Client-Entität den Widerruf eines von ihr angeforderten Zertifikats anfordern. Lautet der Wert 'NONE', kann die Client-Entität den Widerruf eines Zertifikats nicht anfordern.	Any	Nein
[IssuerCrossCertPolicy]			
SigAlg1=	Name des ersten Unterschriftsalgorithmus. Ein entsprechender Eintrag im OID-Abschnitt ist erforderlich.	sha-1WithRSAEncryption	Nein

Tabelle 14. RA-Server - Konfigurationsdatei (Forts.)

Parameter	Beschreibung	Wert gemäß Standardkonfiguration	Nach Konfiguration problemlos änderbar?
StartTimeSpecifiable=	Gibt an, ob der Anfordernde (Client-Entität oder RA) die Startzeit angeben kann.	T	Nein
KeySpecifiable=	Gibt an, ob der Anfordernde (Client-Entität oder RA) den allgemeinen Schlüssel des Zertifikatsgegenstands angeben kann.	T	Nein
KeyUsageSupported=	Gibt an, ob die Erweiterung der Schlüsselverwendung unterstützt wird.	T	Nein
KeyUsageRequired=	Gibt an, ob die Erweiterung der Schlüsselverwendung erforderlich ist.	F	Nein
PolicyCritical=	Gibt an, ob es sich um eine kritische Regel handelt.	F	Nein
PolicyRequired=	Gibt an, ob die Regel erforderlich ist.	F	Nein
PolicyName1=	Der Name der primären Regel. Hierfür muss im OID-Abschnitt eine entsprechende OID vorliegen.	MyPolicy	Nein
Policy1Org=	Der Name des Unternehmens, das diese primäre Regel benötigt.	Ihr Unternehmen	Nein
Policy1Notice1=	Notice1 wird Policy1 zugeordnet.	3	Nein
Policy1Notice2=	Notice2 wird Policy1 zugeordnet.	17	Nein
UserNoticeText1=	Ein juristischer Hinweis oder eine Ablehnungserklärung, die die andere Partei lesen und bei Entscheidungen berücksichtigen muss.	Juristischer Hinweis oder Ablehnungserklärung	Nein
CSP1	URL-Adresse, unter der die Anweisung für Policy1 verfügbar ist.	http://localhost/index.html	Nein
PolicyName2=	Name der sekundären Regel.	My Lite Policy	Nein

Tabelle 14. RA-Server - Konfigurationsdatei (Forts.)

Parameter	Beschreibung	Wert gemäß Standardkonfiguration	Nach Konfiguration problemlos änderbar?
CPS2=	URL-Adresse, unter der die Anweisung für Policy2 verfügbar ist.	http://localhost/index.html	Nein
EERevokeRequests=	Gibt an, ob eine Client-Entität den Widerruf eines Zertifikats anfordern kann. Lautet der Wert 'ANY', kann die Client-Entität den Widerruf eines beliebigen Zertifikats anfordern. Lautet der Wert 'SELF', kann die Client-Entität den Widerruf eines von ihr angeforderten Zertifikats anfordern. Lautet der Wert 'NONE', kann die Client-Entität den Widerruf eines Zertifikats nicht anfordern.	ANY	Nein
[General]			
MyName	Registrierter Name der Entität.	/C=US/O=Ihr Unternehmen/OU=Trust Authority/CN=Trust Authority RA	Nein
Issuer1	Registrierter Name des CA dieser RA.	/C=US/O=Ihr Unternehmen/OU=Trust Authority/CN=Trust Authority CA	Nein
Issuer1URL1	URL-Adresse des CA dieser RA.	pkix://servername:1830	Ja
TempPath=	Pfad zur Speicherung temporärer Dateien.	Für Windows NT: c:\Program Files\IBM\Trust Authority\pkrf\Domains\YourDomain\etc\ Für AIX: /usr/lpp/iau/pkrf/Domains\YourDomain/etc/	Nein
PathToDLLs=	Pfad zur Installation von PKIX-Bibliotheken.	Für Windows NT: c:\pkix\ Für AIX: /usr/pkix/	Nein
TrustChainDelivery=	0 = Übergabe der Trust-Kette ist inaktiviert. 1 = Übergabe der Trust-Kette ist	0 aktiviert.	Ja

Tabelle 14. RA-Server - Konfigurationsdatei (Forts.)

Parameter	Beschreibung	Wert gemäß Standardkonfiguration	Nach Konfiguration problemlos änderbar?
[Transport]			
TCPPort=	TCP-Port, der von der RA überwacht wird.	829	Ja
TCPHost=	TCP/IP-Host-Name der Maschine, auf der sich die RA befindet.	Ihr Host-Name	Nein
PollInterval=	Sendeaufrufintervall.	30s	Ja
RetryInterval=	Die Zeit zwischen den CA-Abfragen durch die RA, sofern der vom CA an die RA übermittelte Zeitpunkt für den Sendeaufruf vor der aktuellen Uhrzeit der RA liegt.	1m	Ja
[KeyStore]			
CurKeyStore=	Momentan verwendeter KeyStore	VSC	Nein
[VSC] Dieser Abschnitt ist erforderlich, wenn der Wert des Parameters 'CurKeyStore' 'VSC' lautet.			
Model=	Art des verwendeten Speichers.	PKCS11_STORAGE_MODEL	Nein
GUID=	Global Unique Identifier.	7F529C80-C942-11D1-8FB0-0004AC61389A	Nein
InitialSOpw=	Anfangskennwort für den Prüfadministrator.	SOPIN	Nein
TokenDir=	Absoluter Pfad und Dateiname für die virtuelle Smart Card.	Für Windows NT: c:\Public Files\IBM\Trust Authority\pkrf\Domains\YourDomain\etc\raKS.fil Für AIX: /usr/lpp/iau/pkrf/Domains/YourDomain/etc/raKS.fil	Nein
[TrustPolicy]			
UseCRLs=	Gibt an, ob CRLs und ARLs als Teil des Prüfprozesses verwendet werden sollen.	T	Nein
AllowExpiredCRLs=	Gibt an, ob abgelaufene CRLs zulässig sind.	F	Nein
AllowFutureCRLs=	Gibt an, ob CRLs mit zukünftigen Datumsangaben zulässig sind.	F	Nein

Tabelle 14. RA-Server - Konfigurationsdatei (Forts.)

Parameter	Beschreibung	Wert gemäß Standardkonfiguration	Nach Konfiguration problemlos änderbar?
AllowExpiredCertificates=	Gibt an, ob abgelaufene Zertifikate zulässig sind.	F	Nein
AllowFutureCertificates=	Gibt an, ob Zertifikate mit zukünftigen Datumsangaben zulässig sind.	F	Nein
ApplyNameConstraintsToEEOnly=	Gibt an, ob Namenseinschränkungen für alle oder nur für das letzte Zertifikat in der Kette angewendet werden sollen.	F	Nein
AllowCRLSearchToFail=	Gibt an, ob ein Fehler vorliegt, wenn keine CRLs oder ARLs für einen Aussteller gefunden werden.	F	Nein
MaximumChainSearchDepth=	Maximale Verkettungstiefe bei rekursiven breitenorientierten Verkettungen	15	Nein
[LDAP]			
NumServers=	Anzahl von LDAP-Servern.	1	Nein
Server1=	Host-Name und Port-Nummer für den LDAP-Server.	hostname:port	Ja
AuthName1	DN des Directory-Administrators	/C=US/O=Ihr Unternehmen/OU=Trust Authority/CN=DirAdmin	Nein
AuthPwd1	Kennwort des Directory-Administrators (nur mit dem Tivoli PKI-Dienstprogramm 'Change Password' ändern)	Secure99	Ja
PostInterval=	Intervall, in dem geprüft wird, ob Informationen zum Senden an das Directory vorliegen.	5m	Ja

Tabelle 14. RA-Server - Konfigurationsdatei (Forts.)

Parameter	Beschreibung	Wert gemäß Standardkonfiguration	Nach Konfiguration problemlos änderbar?
DirectorySchema=	LDAP-Schemaversion 2 oder LDAP Schemaversion 3 verwenden.	3	Ja
[RemoteServer]			
MaxSessions=	Optimierungsparameter.	16	Nein
EncryptionPolicy=	Gibt an, ob für die Verbindung zwischen einem Hintergrund-Server und dessen fernem Administrator eine Verschlüsselungsregel angewendet wird, wenn sich beide auf dem selben System befinden.	F	Nein
NumAdmins=	Anzahl der zertifizierten Administratoren.	0	Nein
Admin1DN=	DN von Administrator1.	Nicht verwendet	Nein
CurrentAdminPort	Aktueller Verwaltungs-Port	Nicht verwendet	Nein
[ICL]			
IclOdbcProvider	Art des ODBC-Anbieters.	UDB	Nein
IclOdbcDriverConnect	Name der Datenbank für ICL.	DSN=pkrfdb	Nein
[URLs]			
/C%EQ%US/O%EQ%Ihr Unternehmen/OU%EQ%Trust Authority/ CN%EQ%Trust Authority CA=pkix://localhost:1830	Dieser Eintrag wird bei der Konfiguration mit der URL-Adresse und dem DN für den CA definiert.	CA DN	Ja

Konfigurationsdatei für Prüfserver

Die Konfigurationsdatei des Prüf-Servers, AuditServer.ini, definiert die Konfigurationsvariablen des Prüf-Servers. Diese Variablen konfigurieren die grundlegenden Funktionsmerkmale des Servers und definieren das Protokollieren von Debug- und Fehlernachrichten. Die Variablen legen außerdem fest, welche Ereignisse protokolliert werden. Die nachfolgenden Abschnitte enthalten zusätzliche Informationen zu den Einträgen in Tabelle 15 auf Seite 106.

- Generische Parameter von Servicesteuerroutinen
- Bewertungsstufen für Ereignisse
- Trace-Stufen

Generische Parameter von Servicesteuerroutinen

Folgende Parameter für Servicesteuerroutinen können für jeden Service verwendet werden:

- service.count - Die Anzahl verfügbarer Services
- service.x.name - Der Name eines Services
- service.x.classname - Der Klassenname eines Services
- service.x.dpolicy - Der Klassenname einer Übergaberegel
- service.default.count - Die Anzahl der Standardservices
- service.default.x.name - Der Name eines Standardservices

Trace-Stufen

Es existieren folgende Trace-Stufen:

- All - Protokollierung von Fehler-, Warnungs-, Informations- und Trace-Nachrichten
- Error - Protokollierung von Fehlernachrichten
- Warning - Protokollierung von Fehlernachrichten und Warnungen
- Eventinfo - Protokollierung von Fehler- und Trace-Nachrichten
- None - Keine Protokollierung von Nachrichten

Tabelle 15. Prüf-Server - Konfigurationsdatei

Parameter	Beschreibung	Standardwert	Nach Konfiguration problemlos änderbar?
Server-Port			
acceptor.classname=	Der Name der Acceptor-Klasse.	com.ibm.irg.sysmgmt.daemon.acceptors.SMSocketAcceptor	Nein
acceptor.arg=	Der Port, der vom Prüf-Server überwacht wird.	7222	Ja
acceptor.init.retries=	Anzahl der Bindungsversuche am Server-Socket	3	Ja
acceptor.init.delay=	Die Anzahl an Sekunden, die zwischen zwei Bindungsversuchen gewartet werden soll. (Das Programm geht von Sekunden aus.)	3	Ja
Servicesteuerroutine			
service.count=	Die Anzahl verfügbarer Services	2	Nein
Protokollservice			
service.1.name=	Der Name des Protokollservices	log	Nein
service.1.classname=	Der Klassenname des Protokollservices	com.ibm.irg.sysmgmt.daemon.services.log.SMLogService	Nein
service.1.dpolicy=	Der Klassenname der Übergaberegel des Protokollservice.	com.ibm.irg.sysmgmt.daemon.services.log.SMLogDeliveryPolicy	Nein
Prüfservice			
service.2.name=	Der Name des Prüfservices	audit	Nein
service.2.classname=	Der Klassenname des Prüfservices	com.ibm.irg.sysmgmt.daemon.services.audit.SMAuditService	Nein
service.2.dpolicy=	Der Klassenname der Übergaberegel des Prüfservices	com.ibm.irg.sysmgmt.daemon.services.audit.SMAuditDeliveryPolicy	Nein
Standardservices			
service.default.count=	Die Anzahl verfügbarer Standardservices	2	Nein
service.default.1.name=	Der Name des Standardservices	log	Nein
service.default.2.name=	Der Name des Standardservices	audit	Nein
Ereigniskonfiguration			
irgsmd.event.config=	Die Ereigniskonfigurationsdatei	smevents.conf	Nein

Tabelle 15. Prüf-Server - Konfigurationsdatei (Forts.)

Parameter	Beschreibung	Standardwert	Nach Konfiguration problemlos änderbar?
Konfiguration des Protokollservices			
event.log.filename=	Die Datei zur Aufzeichnung von Ereignissen.	Für Windows NT: c:\\Program Files\\IBM\\Trust Authority\\logs\\smevents.log Für AIX: /usr/lpp/iau/logs/smevents.log	Ja
event.log.append=	Markierung, die angibt, ob Daten an das Ereignisprotokoll angefügt werden oder ob dieses überschrieben wird.	true	Ja
event.log.severity.min=	Mindestbewertung für Ereignisprotokoll	1	Ja
event.log.severity.max=	Maximale Bewertung für Ereignisprotokoll	7	Ja
Servicekonfiguration			
audit.ksfile=	Die KeyStore-Prüfdatei. Diese Datei wird zum Speichern der Prüf-Chiffrierschlüssel verwendet.		Nein
audit.catalog	Der Dateiname der NLS-Katalogdatei.	Für Windows NT: c:\\Program Files\\IBM\\Trust Authority\\catalog\\IRGVDS.DLL Für AIX: /usr/lpp/iau/catalog/IRGVDS.cat	Nein
audit.db.instance=	Der Name des DB2-Prüfexemplars.		Nein
audit.db.name=	Der Name der Prüfdatenbank.		Nein
audit.db.connection=	Der Algorithmus zur Verwaltung der Datenbankverbindung.	single	Nein
audit.log.connect.retries=	Die Anzahl der zulässigen Versuche zur Herstellung einer Verbindung zur Datenbank/Protokolldatei.	3	Ja
audit.log.update.retries=	Die Anzahl der zulässigen Versuche zur Aktualisierung des Prüfprotokolls.	3	Ja

Tabelle 15. Prüf-Server - Konfigurationsdatei (Forts.)

Parameter	Beschreibung	Standardwert	Nach Konfiguration problemlos änderbar?
audit.log.timeout	Der zulässige Zeitlimitüberschreitungswert zur Aktualisierung des Prüfprotokolls.	60s	Ja
audit.log.integrity=	Aktivieren oder Inaktivieren der Integritätsprüfung.	true	Nein
Trace			
trace.enable=	Eine Markierung zur Aktivierung/Inaktivierung der Trace-Funktion.	false	Ja
trace.level.name=	Der Name für eine Trace-Stufe	all	Ja
trace.event.enable=	Aktivieren/Inaktivieren der Trace-Funktion für Ereignisse	false	Nein
trace.log.filename=	Der Name der Trace-Protokolldatei.	Für Windows NT: c:\\Program Files\\IBM\\Trust Authority\\logs\\iausmd.log Für AIX: /usr/lpp/iau/logs/iausmd.log	Ja
trace.log.append=	Markierung, die angibt, ob Daten an die vorhandene Trace-Datei angefügt werden	true	Ja
Fehler			
error.log.filename=	Der Name der Fehlerdatei.	Für Windows NT: c:\\Program Files\\IBM\\Trust Authority\\logs\\iausmd.err Für AIX: /usr/lpp/iau/logs/iausmd.err	Ja

Konfigurationsdatei für Prüf-Client

Die Konfigurationsdatei des Prüf-Clients, AuditClient.ini, definiert die Konfigurationsvariablen des Prüf-Clients.

Tabelle 16. Prüf-Client - Konfigurationsdatei

Parameter	Beschreibung	Standardwert	Nach Konfiguration problemlos änderbar?
Verbindungseinstellungen			
[CONNECTION]			
EnableAudit=	Aktivieren/Inaktivieren von Prüfereignissen	true	Nein
HostName=	Prüf-Server-Host	*Ihr Host-Name*	Nein
Port=	Port des Prüf-Servers. Muss mit dem in der Datei 'AuditServer.ini' angegebenen Port übereinstimmen.	59998	Ja
AuthType=	Authentifizierungsmechanismus. Dieser Parameter wird in diesem Release von Tivoli PKI nicht unterstützt.	Keiner	Nein
UseSSL=	Soll SSL für die Client/Server-Sitzung verwendet werden? Für zukünftige Sitzungen. Dieser Parameter wird in diesem Release von Tivoli PKI nicht unterstützt.	Nein	Nein
SSLKeyDB=	SSL-Schlüsseldatenbank. Dieser Parameter wird in diesem Release von Tivoli PKI nicht unterstützt.	Für AIX: /usr/lpp/iau/audit/client/ssl.kdb Für Windows NT: c:\Program Files\IBM\Trust Authority\audit\client\ssl.kdb	Nein
SSLv2Token=	SSL-Schlüsseldatenbank-Token. Dieser Parameter wird in diesem Release von Tivoli PKI nicht unterstützt.	Token	Nein
Retries=	Anzahl von Sendeversuchen für ein Ereignis	4	Ja
Timer	Die Zeit in Millisekunden, die zwischen den Wiederholungsversuchen für das Herstellen einer Verbindung zum Server gewartet werden soll.	1000	Ja

Tabelle 16. Prüf-Client - Konfigurationsdatei (Forts.)

Parameter	Beschreibung	Standardwert	Nach Konfiguration problemlos änderbar?
Abschnitte für Komponentenmasken			
[CA]			
ExcludedEvents=	CA-Ereignisse, die nicht gesendet werden		Ja
[RA]			
ExcludedEvents=	RA-Ereignisse, die nicht gesendet werden	ReceiptOfCertRequest	Ja

Befehlszeilendienstprogramme

Dieser Abschnitt enthält Beschreibungen der Syntax und der Parameter für folgende Befehlszeilendienstprogramme:

- Dienstprogramm CA Certification
- Dienstprogramm Add RA User
- Dienstprogramm Enable RA Encryption
- Dienstprogramm Audit Archive and Sign
- Dienstprogramm Audit Integrity Check
- Dienstprogramm Create New RA
- Dienstprogramm Multiple RA Authorization
- Dienstprogramm Bulk Certificate Issuance
- Dienstprogramm CA Key Update

Dienstprogramm CA Certification

Mit dem Dienstprogramm CA Certification können Sie von einem anderen CA Zertifizierungen für den Tivoli PKI-CA anfordern. Hierzu stehen Ihnen das Modell zur gegenseitigen Zertifizierung und das hierarchische Sicherungsmodell zur Verfügung.

Anmerkung: Wenn Sie im Rahmen Ihrer Gesamthierarchielösung die hierarchischen CA-Zertifikate in Netscape Communicator herunterladen, verwenden Sie den Parameter '-m ..' mit dem Dienstprogramm CA Certification. Durch die Verwendung des Parameters '-m..' wird die Erweiterung für Namenseinschränkungen (Name Constraints) aus dem resultierenden CA-Zertifikat ausgeschlossen. Das Exemplar eines solchen Befehls könnte beispielsweise folgendermaßen aussehen:

```
CACertRq -m .. -h -r "c:\Program Files\IBM\Trust Authority\ccprereg.reg"
   -P 1835 -W Secure99
```

Verwenden Sie mit dem Dienstprogramm CA Certification keine der folgenden Befehlszeilenoptionen für Namenseinschränkungen:

- -i oder -I
- -d oder -D
- -u oder -U
- -n oder -N
- -m oder -M

Syntax

Die Syntax für dieses Dienstprogramm lautet wie folgt:

```
CACertRq
    [-i ipAddressMask [-I ipAddressMask]]
    [-d dns [-D dns]]
    [-m emailAddress [-M emailAddress]]
    [-u uri [-U uri]]
    [-n directoryName [-N directoryName]]
    [-p inhibitPolMap]
    [-h [-m ..]]
    [-H filename -e | -E]
    [-C filename | -B
filename]
```

```
[-S filenames]
-r preregistrationpath
-P 1835
-W password
```

Parameter

[-i *ipAddressMask* **[-I** *ipAddressMask***]]**
Die IP-Adressmaske (IP = Internet Protocol) im CDIF-Format. Der kleingeschriebene Parameter (-i) fügt die angegebene IP-Adressmaske der Liste zulässiger Unterverzeichnisstrukturen hinzu. Der großgeschriebene Parameter (-I) entspricht dem kleingeschriebenen Parameter. Die angegebene IP-Adressmaske wird jedoch der Liste unzulässiger Unterverzeichnisstrukturen hinzugefügt.

Die Maske des Unternehmens X lautet beispielsweise 9.0.0.0/255.0.0.0 und die der Abteilung Y dieses Unternehmens lautet 9.210.134.0/255.255.254.0.

[-d *dns* **[-D** *dns***]]**
Die Adresse des Domain Name Server (DNS). Der kleingeschriebene Parameter (-d) fügt die angegebene DNS-Adresse der Liste zulässiger Unterverzeichnisstrukturen hinzu. Der großgeschriebene Parameter (-D) entspricht dem kleingeschriebenen Parameter. Die angegebene DNS-Adresse wird jedoch der Liste unzulässiger Unterverzeichnisstrukturen hinzugefügt.

Beginnt die Adresse mit einem Punkt, werden alle Hosts einbezogen, die mit dieser Unterzeichenfolge (einschließlich '.') enden. Ist dies nicht der Fall, wird nur der Host einbezogen, der der Zeichenfolge entspricht.

Der Einschränkung '.orga.com' entsprechen beispielsweise die Hosts us.orga.com, vneto-.orga.com und w3.software.orga.com, jedoch nicht orga.com selbst oder kidorga.com. Der Einschränkung orga.com entspricht der Host orga.com, jedoch nicht us.orga.com oder die anderen. Daraus folgt, dass eine zulässige Unterverzeichnisstruktur ohne führenden Punkt nur einen möglichen Knoten angibt.

[-m *emailAddress* **[-M** *emailAddress***]]**
Die E-Mail-Adressen. Der kleingeschriebene Parameter (-m) fügt die angegebene E-Mail-Adresse der Liste zulässiger Unterverzeichnisstrukturen hinzu. Der großgeschriebene Parameter (-M) entspricht dem kleingeschriebenen Parameter. Die angegebene E-Mail-Adresse wird jedoch der Liste unzulässiger Unterverzeichnisstrukturen hinzugefügt.

Eine E-Mail-Adresse kann im Standardformat (ohne Platzhalter) oder als DNS-Adresse angegeben werden. Die Regeln für eine DNS-Adresse entsprechen den Regeln für die Option -d. Daraus folgt, dass eine zulässige Unterverzeichnisstrukturen mit einer Standard-E-Mail-Adresse nur einen möglichen Benutzer angibt.

[-u *uri* **[-U** *uri***]]**
Die URI. Der kleingeschriebene Parameter (-u) fügt die angegebene URI der Liste zulässiger Unterverzeichnisstrukturen hinzu. Der großgeschriebene Parameter (-U) entspricht dem kleingeschriebenen Parameter. Die angegebene URI wird jedoch der Liste unzulässiger Unterverzeichnisstrukturen hinzugefügt.

Der Knotenabschnitt der URI (Uniform Resource Identifier) unterliegt den gleichen Regeln wie die Option -d, sofern er keine IP-Adresse enthält. In diesem Fall wird er als exakte Übereinstimmung behandelt.

[-n *directoryName* **[-N** *directoryName***]]**
Der Directory-Name. Der kleingeschriebene Parameter (-n) fügt das angegebene Directory der Liste zulässiger Unterverzeichnisstrukturen hinzu. Der großgeschriebene Parameter (-N) entspricht dem kleingeschriebenen Parameter. Das angegebene Directory wird jedoch der Liste unzulässiger Unterverzeichnisstrukturen hinzugefügt.

Diese Namen müssen im LDAP-Standardformat angegeben werden. Namen, die dem Ende der angegebenen RDNs (Relative Distinguished Names) entsprechen, gelten als exakte Übereinstimmung, auch wenn andere RDNs vorhanden sind.

Anmerkung: Wenn Sie als Parameter eines Befehls einen Verzeichnispfad angeben, der eingebettete Leerzeichen enthält, müssen Sie den Pfad in doppelte Anführungszeichen (″ ″) setzen.

[-h]
Gibt an, dass die Zertifikatsanforderung das hierarchische Sicherungsmodell verwendet.

[-H *filename***]**
Erstellt eine Antwortdatei im PKCS#7-Format für einen Fremd-CA. Auf diese Weise wird eine Abwärtshierarchie erstellt.

[-m ..]
Gibt an, dass die Erweiterung für Namenseinschränkungen (Name Constraints) aus dem Zertifikat ausgeschlossen wird.

[-C *filename***]**
Gibt den Namen der Datei an, in die die binärcodierte Anforderung PKCS#10 geschrieben wird. Die Parameter '-C' und '-B' schließen sich gegenseitig aus.

[-B *filename***]**
Gibt den Namen der Datei an, in die die Base 64-binärcodierte Anforderung PKCS#10 geschrieben wird. Die Parameter '-C' und '-B' schließen sich gegenseitig aus.

[-S *filename***]**
Gibt den Namen der Datei an, die die Antwort für PKCS#7 enthält.

[-e | -E]
In Kombination mit dem Parameter '-H' geben diese Parameter an, in welchem Format die Antwortdatei erstellt werden soll (Binär- oder base64-Format). Bei Verwendung des Parameters '–e' wird die Antwortdatei im Binärformat erstellt, bei Verwendung des Parameters '–E' wird sie im base64-Format erstellt.

[-E]

-r *preregistrationpath*
Der Pfadname der vom ausstellenden System erzeugten Vorabregistrierungsdatei.

-P 1835
Die administrative Port-Nummer des CA (1835).

-p *inhibitPolMap*
Der Wert des Erweiterungsfelds 'inhibitPolicyMapping'.

Ist diese Option nicht vorhanden, lautet der Standardwert 1.

-W *password*
Das bei der Erzeugung der Vorabregistrierungsdatei eingegebene Kennwort.

Dienstprogramm Add RA User

Mit dem Dienstprogramm Add RA User können Sie der angegebenen Tivoli PKI-Registrierungsdomäne einen administrativen RA-Benutzer (oder einen Registrator) hinzufügen.

Anmerkung: Wenn Sie als Parameter eines Befehls einen Verzeichnispfad angeben, der eingebettete Leerzeichen enthält, müssen Sie den Pfad in doppelte Anführungszeichen (″ ″) setzen.

Syntax

```
add_rauser domain_configuration_file domain_name ID
[access_profile]
```

Parameter

domain_configuration_file
Der absolute Pfad zur Domänenkonfigurationsdatei (domain.cfg). Diese Datei enthält einen Abschnitt für jede im System konfigurierte Registrierungsdomäne. Auf diese Weise können Sie das virtuelle Stammverzeichnis der angegebenen Registrierungsdomäne lokalisieren.

domain_name
Der Name der Registrierungsdomäne, die der hinzugefügte Registrator verwalten soll.

ID Entweder die vom Browser zum Zeitpunkt der Zertifikatsanforderung an den Benutzer zurückgegebene ID oder die Identitätsnachweis-UUID, die Sie erhalten, wenn Sie mit Hilfe von RA Desktop den Zertifikatseintrag des Benutzers anzeigen.

Wenn Sie den Parameter für die ID angeben, geht das Programm zunächst davon aus, dass es sich bei der ID um eine Anforderungs-ID handelt. Es verwendet anschließend diesen Wert, um die Identitätsnachweis-UUID festzustellen (beispielsweise `sp0ApHvpzvCicr1Ts8ssKw==`). Das Zertifikat muss also bereits zuvor an den Benutzer ausgestellt worden sein, der die Berechtigung als Registrator anfordert.

Kann kein übereinstimmender Eintrag in der Registrierungsdatenbank gefunden werden, geht das Programm davon aus, dass es sich bei der ID um eine Identitätsnachweis-UUID handelt. Es versucht, einen entsprechenden Anforderungseintrag zu finden. Kann keine Übereinstimmung gefunden werden, gibt das Programm eine Warnung aus und versucht, einen Eintrag zur Tabelle der Registratoren (rausers) in der Datenbank hinzuzufügen.

access_profile
Ein optionaler Parameter, der das Zugriffsprofil angibt, das dem Registrator zugeordnet ist, den Sie dem System hinzufügen. Wenn Sie keinen Wert angeben, verwendet das Programm den Standardwert RAUser.

Bei diesem Parameter muss es sich um ein gültiges Profil handeln, das in einer der Tivoli PKI-Konfigurationsdateien für die Registrierungsverwaltung angegeben wurde. Das Profil enthält die Anforderungsarten, Aktionen etc., die die zugeordneten Registratoren ausführen können.

Dienstprogramm Enable RA Database Encryption

Standardmäßig werden Informationen in der Datenbank der Registrierungseinrichtung nicht verschlüsselt. Nach der Konfiguration können Sie die Datenbankverschlüsselung durch Ausführen des Programms Enable RA Database Encryption (iauEnableRADBSec) aktivieren.

Syntax

```
iauEnableRADBSec -d domain_name -r install_directory [i]
```

Parameter

-d *domain_name*
Der Name Ihrer Registrierungsdomäne. Dieser Wert muss mit dem Wert übereinstimmen, der im Setup Wizard für den Registrierungsdomänennamen angegeben wurde.

-r *install_directory*
Der vollständige Pfad, unter dem Tivoli PKI installiert ist.

-i *install_directory*
Ein optionaler Parameter, über den das System angewiesen wird, Debug-Nachrichten (derzeit nur in Englisch) anzuzeigen.

Dienstprogramm Audit Archive and Sign

Mit dem Dienstprogramm Audit Archive and Sign können Sie Prüfprotokolldateien archivieren und unterzeichnen.

Anmerkung: Wenn Sie als Parameter eines Befehls einen Verzeichnispfad angeben, der eingebettete Leerzeichen enthält, müssen Sie den Pfad in doppelte Anführungszeichen (″ ″) setzen.

Syntax

```
AuditArchiveAndSign [-c ConfigFile Path] [-n] ArchiveFileName
```

Parameter

-c *ConfigFilePath*
Der absolute Pfad der Konfigurationsdatei des Prüf-Servers.

- Der Standardpfad für AIX lautet: /usr/lpp/iau/etc/TrustAuthority/AuditServer.ini
- Der Standardpfad für Windows NT lautet: c:\Program Files\IBM\Trust Athority\etc\TrustAuthority\AuditServer.ini

Anmerkung: Dieser Parameter ist optional. Wenn Sie keinen Wert angeben, wird die Standardkonfigurationsdatei des Prüf-Servers angegeben.

-n Gibt an, dass Protokolleinträge nicht aus der Datenbank gelöscht werden sollen.

ArchiveFileName
Das Namenspräfix der Datei, in die die Prüfprotokolle geschrieben werden. Das Dienstprogramm fügt den Archiv- und Unterschriftsdateien die Endungen .ixf beziehungsweise .sig hinzu.

Dienstprogramm Audit Integrity Check

Das Dienstprogramm Audit Integrity Check prüft die Integrität von Protokolleinträgen sowohl in Archiven als auch in der Datenbank des Prüf-Servers. Dieses Tool kann nur dann eingesetzt werden, wenn Integritätsprüfungen auf Ihrem System aktiviert wurden. Die Syntaxformate für diesen Befehl lauten wie folgt:

- Format 1

  Dieses Format prüft die Integrität der Datenbank des Prüf-Servers und fordert Sie zur Eingabe des Prüfadministratorkennworts auf.

- Format 2

  Diese Format prüft die Integrität einer oder mehrerer Archivdateien des Prüf-Servers und fordert Sie zur Eingabe des Prüfadministratorkennworts auf.

- Format 3

  Dieses Format prüft die Integrität aller Archivdateien im angegebenen Verzeichnis und fordert Sie zur Eingabe des Prüfadministratorkennworts auf.

Anmerkung: Wenn Sie als Parameter eines Befehls einen Verzeichnispfad angeben, der eingebettete Leerzeichen enthält, müssen Sie den Pfad in doppelte Anführungszeichen (″ ″) setzen.

Syntax

Format 1:

```
AuditIntegrityCheck [-c ConfigFilePath] -d
```

Format 2:

```
AuditIntegrityCheck [-c ConfigFilePath] -a ArchiveFileName1 ArchiveFileName2
ArchiveFileName3
```

Format 3:

```
AuditIntegrityCheck [-c ConfigFilePath] -A ArchiveFileDirectory
```

Parameter

-c *ConfigFilePath*

Der absolute Pfad der Konfigurationsdatei des Prüf-Servers.

- Der Standardpfad für AIX lautet: /usr/lpp/iau/etc/TrustAuthority/AuditServer.ini
- Der Standardpfad für Windows NT lautet: c:\Program Files\IBM\Trust Authority\etc\TrustAuthority\AuditServer.ini

Anmerkung: Dieser Parameter ist optional. Wenn Sie keinen Wert angeben, wird die Standardkonfigurationsdatei des Prüf-Servers angegeben.

-a *ArchiveFileName1 ArchiveFileName2 ArchiveFileName3*

Das Pfadnamenpräfix der Archivdateien, deren Integrität geprüft werden soll. Das Präfix steht für eine Gruppe von Dateien, die dem Archiv zugeordnet sind.

Der Befehl '-a /local/archive/archive1-1067' verarbeitet beispielsweise mehrere Dateien mit dem Pfadnamenpräfix '/local/archive/archive1-1067' wie folgt:

```
/local/archive/archive1-1067_audit_log.ixf
/local/archive/archive1-1067_audit_log.sig
```

-A *ArchiveFileDirectory*

Der Pfadname des Verzeichnisses, das die Archivdateien enthält, deren Integrität geprüft werden soll. Alle Dateien mit den Endungen _audit_log.ixf und _audit_log.sig werden geprüft.

Dienstprogramm Create New RA

Mit dem Dienstprogramm Create New RA werden mehrere RAs (MRA) definiert. Das Dienstprogramm Create New RA erstellt eine Datendatei, die vom Setup Wizard verwendet wird, um die MRA einzurichten. Das Dienstprogramm erstellt die Datendatei anhand einer Schablonendatei namens 'mraTemplate.ini'. Dieses Dienstprogramm wird auf dem CA-Server ausgeführt.

Syntax

```
createNewRA [-f filename]
```

Parameter

-f *filename*
’filename’ steht für den Namen der Datendatei.

Anmerkung: Dieser Parameter ist optional. Wenn Sie keinen Wert angeben, lautet der Name der Datendatei ’mraConfig.dat’.

Dienstprogramm Multiple RA Enrollment Authorization

Mit dem Dienstprogramm Multiple RA Enrollment Authorization wird eingesetzt, wenn mehrere RAs (MRA) eingerichtet werden. Es liest die während der MRA-Einrichtung erstellte Vorabregistrierungsdatei und berechtigt die neue MRA. Auf diese Weise kann der CA alle durch die MRA ausgestellten Zertifikate unterzeichnen, sobald die Einrichtung abgeschlossen wurde. Dieses Dienstprogramm wird auf dem CA-Server ausgeführt.

Syntax

```
authRAEnrollment -f filename
```

Parameter

-f *filename*
Gibt den Namen der Datei an, die zur Registrierung der MRA verwendet wird.

Anmerkung: Dieser Parameter ist optional. Wenn Sie keinen Wert angeben, lautet der Name der Datendatei ’mraConfig.dat’.

Dienstprogramm Bulk Certificate Issuance

Das Dienstprogramm Bulk Certificate Issuance (BCI) bietet für einen RA-Administrator eine sichere Methode, um mehrere digitale Zertifikate durch eine einzige Anforderung an Tivoli PKI anzufordern.

BCI kann durch einen RA-Administrator auf einem RA-Server ausgeführt werden, der mit dem benannten Tivoli PKI-System verbunden ist. Der Administrator muss eine BCR-Datei (Bulk Certificate Request - Massenzertifikatsanforderung) zur Verfügung stellen. Die BCR-Datei enthält eine Reihe von Datensätzen, die jeweils eine eindeutige Kunden-ID zusammen mit dem öffentlichen Schlüssel oder der PKCS#10-Zeichenfolge enthalten. Außerdem beinhalten diese Datensätze weitere Informationen, die zur Ausstellung des digitalen Zertifikats für diesen Kunden benötigt werden. Bei der Ausstellung von digitalen Zertifikaten generiert BCI eine PKCS#7-Zeichenfolge für jedes Zertifikat und speichert die Zeichenfolge in der Datenbank ’pkrf’ des benannten Tivoli PKI-Systems. Die PKCS#7-Zeichenfolgen enthalten das Zertifikat und die CA-Zertifikatketten. BCI stellt die Zertifikate und die Ketten im PKCS#7-Format mit der entsprechenden Kunden-ID aus.

Anforderungsdatei für Massenzertifikat erstellen

Für die Erstellung der BCR-Datei (Bulk Certificate Request - Massenzertifikatsanforderung) ist der Administrator zuständig. Die BCR-Datei ist eine Texteingabedatei für BCI, die für jede Zertifikatsanforderung einen Datensatz enthält. Jeder Datensatz enthält wiederum die Paare aus den Schlüsselnamen und Werten für die Informationen, die bei jeder Anforderung benötigt werden. Jeder neue Datensatz in dieser Datei beginnt mit dem Schlüsselnamen **PREID**.

Gültige Schlüsselnamen:

BATCHID=*x*;
Die eindeutige ID für einen Stapel von BCI-Anforderungen. Sie können die Stapel-ID in jedem gewünschten Format angeben.

PREID=*x*;
Die kundendefinierte ID für die Anforderung.

CERTTYPE=*x*;
Der Zertifikatstyp für dieses Zertifikat. Alle nachfolgenden Einträge in diesem Stapel verwenden denselben Wert für **CERTTYPE**, bis ein neuer Wert für **CERTTYPE** angegeben ist. Der Standardzertifikatstyp lautet **SSLBrowserCert1Year**.

LASTNAME=*x*;
Der Nachname der Person, für die das Zertifikat angefordert wird.

FIRSTNAME=*x*;
Der Vorname der Person, für die das Zertifikat angefordert wird.

EMAILADR=*x*;
Die E-Mail-Adresse der Person, für die das Zertifikat angefordert wird.

COMMNAME=*x*;
Der allgemeine Name für das Zertifikat. (Diese Angabe ist optional.)

ORGNAME=*x*;
Der Name des Unternehmens. (Diese Angabe ist optional.)

ORGUNIT=*x*;
Der Name der Unternehmensabteilung. (Diese Angabe ist optional.)

STREET=*x*;
Die Hausanschrift des Unternehmens. (Diese Angabe ist optional.)

LOCALITY=*x*;
Die Stadt, in der das Unternehmen seinen Sitz hat. (Diese Angabe ist optional.)

STATE=*x*;
Die Name der Region bzw. des Verwaltungsbezirks, in dem/der das Unternehmen ansässig ist. (Diese Angabe ist optional.)

COUNTRY=*x*;
Der Name des Landes, in dem das Unternehmen seinen Sitz hat. (Diese Angabe ist optional.)

DOMAIN=*x*;
Der Domänenname. (Diese Angabe ist optional.)

PKCS10=*x*;
Die PKCS#10-Zeichenfolge im B64-Textformat. Diese PKCS#10-Anforderung muss einen öffentlichen RSA-Schlüssel enthalten.

PUBKEY=*x*;
Die hexadezimal codierte Bitfolge für den öffentlichen Schlüssel im ASN1-Format. Es muss sich hierbei um einen öffentlichen RSA-Schlüssel handeln.

Anmerkungen:

1. Alle in der BCR-Datei aufgelisteten Schlüsselnamen müssen das oben dargestellte Format verwenden.

2. Schlüsselnamen müssen in Großbuchstaben angegeben werden.
3. Alle Schlüsselwerte müssen mit einem Semikolon (;) enden.
4. Die Werte für alle Schlüsselnamen müssen im ASCII-Format angegeben werden und dürfen höchstens 64 Zeichen lang sein (Ausnahmen: **PUBKEY** und **PKCS10**).

Die Schlüsselnamen, die unbedingt angegeben werden müssen, sind **BATCHID**, **PREID**, **LASTNAME**, **FIRSTNAME**, **PKCS10** und **PUBKEY**. Der Schlüsselname **DOMAIN** ist dann erforderlich, wenn **CERTTYPE=IPSecCert1Year** oder **CERTTYPE=IPSecCert2Year** angegeben wird. Alle anderen Schlüsselnamen sind optional. Die Schlüsselnamen müssen nicht in einer bestimmten Reihenfolge angegeben werden. Der Schlüsselname **PREID** wird jedoch als Begrenzer verwendet und signalisiert, dass ein neuer Anforderungssatz beginnt. Daher muss er am Anfang eines Datensatzeintrags stehen.

Beispiel einer Anforderungsdatei für Massenzertifikate

Im Folgenden ist ein Beispiel einer Anforderungsdatei für ein Massenzertifikat (BCR-Datei) dargestellt. Das Beispiel veranschaulicht die gültigen Schlüsselnamen und einige Beispielwerte.

```
BATCHID=Test20010110002;
PREID=100002151;
CERTTYPE=SSLBrowserCert1Year;
LASTNAME=Wang;
FIRSTNAME=wesamy;
EMAILADR=wewang@tivoli.com;
COMNAME=weswang;
ORGNAME=Tivoli;
ORGUNIT=TEST;
STREET=12000 Main Street;
LOCALITY=Austin;
STATE=Texas;
COUNTRY=US;
DOMAIN=play.com;
PUBKEY=30818A02818100E2A31748E2A803437F3831319329A7E9EFA8D35A3B1B79212C
FC0B71F4046DC287F1C28BE4A22879CD2708BCE4C395FC480318E2FF02871E219E51BEF5
320A1E03241E9D0FD21C893E72ECD41F149678C24E0FBC3B69628D9E51613F6049C3CC2D
20F84740ED29F739F73CD5C4C4FD36C71DEC27ABDBE79F98801889129EF8B7020400010001;
PREID=100002152;
CERTTYPE=SSLBrowserCert2Year;
LASTNAME=Tang;
FIRSTNAME=ranny;
EMAILADR=rtang@tivoli.com;
COMNAME=rantang;
ORGNAME=Tivoli;
ORGUNIT=TEST2;
STREET=12004 Main Street;
LOCALITY=BocaRaton;
STATE=Florida;
COUNTRY=US;
DOMAIN=try.com;
PUBKEY=30818A02818100E7348549F8F2EB4BAB01924B47C4D3C00C036BBB1A65C7D12C
BC3AB2DEC9C3D8D8E68FFE2D5D47BB1CD809DEC274FE18EB9A37A4ECC13BE77C6413DC35
D47041AD9088048C5912CFF6A7C971CDB67BBEA5EB6F9B77744B296B06BB00DD50E6E23E
9FC221A105738C610BA325091E251DF7007C4A6FFA38E20AB52B81F397D1A3020400010001;
```

BCI ausführen

BCI wird über die AIX-Befehlszeile ausgeführt. Hierzu müssen Sie als **cfguser** angemeldet sein. Alle BCI-Befehle sind im Verzeichnis '/usr/lpp/iau/bin/' installiert. Um die BCI-Befehle ausführen zu können, müssen Sie zunächst in das Verzeichnis '/usr/lpp/iau/bin/' wechseln.

Der BCI-Prozess besteht aus mehreren Abschnitten. Sie können den gesamten BCI-Prozess über einen einzigen Befehl ausführen oder aber bestimmte BCI-Abschnitte mit unterschiedlichen Befehlen ausführen. Um den gesamten BCI-Prozess als einen Befehl auszuführen, verwenden Sie den Befehl **bcistart**. Sollen die BCI-Befehle separat ausgeführt werden, verwenden Sie hierbei die folgende Reihenfolge:

1. **bciin**
2. **bcirunstart**
3. **bcipost**
4. **bcireport**

Die Befehle für BCI werden im Folgenden beschrieben.

BCI-Befehle

Dieser Abschnitt enthält Beschreibungen der Syntax und der Parameter für die folgenden BCI-Befehlszeilendienstprogramme:

- **bciin**
- **bcirunstart**
- **bcipost**
- **bcireport**
- **bcistart**

Befehl 'bciin'

Bei der Ausführung liest der Befehl **bciin** die Informationen in der BCR-Datei und speichert sie in der Datenbank 'pkrf' auf dem RA-Server. Die Daten aus der BCR-Datei werden so formatiert, dass pro Kundensatz in der Datei 1 Zertifikatsanforderung erstellt wird. Bei jedem Datensatz werden Paare aus Schlüsselnamen und Werten untersucht und die erforderlichen Felder geprüft. Falls ein Fehler festgestellt wird, wird die Anforderung übersprungen, und die Informationen werden in die Protokolldatei geschrieben. Der Prozess wird gestoppt und schreibt einen Fehler in die Protokolldatei, wenn die BCR-Datei nicht gefunden oder nicht gelesen werden kann.

Syntax

Die Syntax dieses Befehls lautet wie folgt:

```
bciin [bcrf]
```

Parameter

bcrf

Der Name der BCR-Datei, die verarbeitet werden soll. Wenn sich die BCR-Datei nicht in demselben Verzeichnis wie der Befehl **bciin** befindet, muss der vollständige Pfad der BCR-Datei angegeben werden.

Beispiel

```
bciin /usr/bcrf/northbank01142001.txt
```

Befehl 'bcirunstart'

Der Befehl **bcirunstart** ruft die Routine **bcirun** auf, die die Zertifikatsanforderungen generiert, sie an den CA sendet und die PKCS#7-Zeichenfolge für die zurückgegebenen Zertifikate erstellt. Die Routine **bcirun** zeichnet den Status der Zertifikatsanforderungen in der

Tabelle für BCI-Anforderungen (BCIRT) der Datenbank PKRF auf, die Sie jederzeit mit dem Befehl **bcireport** anzeigen können. Falls die Anforderung zurückgewiesen wird, wird ihr Status auf **BCIREJECTED** gesetzt. Sind die Daten des öffentlichen Schlüssels falsch, wird der Status auf **BCIPUBLICKEYERROR** gesetzt.

Syntax

Die Syntax dieses Befehls lautet wie folgt:

```
bcirunstart [batchID] [TPKI password]
```

Parameter

batchID
Die Stapel-ID, die als Wert für den Parameter **BATCHID=** in der BCR-Datei angegeben wurde.

TPKI password
Das TPKI-Kennwort ist das Steuerungskennwort für das Tivoli PKI-System.

Beispiel

```
bcirunstart BCI200101140043 adpass23
```

Befehl 'bcipost'

Bei der Ausführung nimmt der Befehl **bcipost** zwei Arten von Sendevorgängen für die angeforderten Zertifikate vor. Bei der ersten Art wird jeder gültige Datensatz aus der Tabelle mit den BCI-Anforderungen (BCIRT) an die Anforderungstabelle in der Datenbank PKRF auf dem RA-Server gesendet. Die zweite Sendeart sendet die Zertifikatsanforderungen an den LDAP-Server. Alle in diesem Prozess gegebenenfalls auftretenden Fehler werden an die Datei 'bcipost.log.*' gesendet (* steht für die Stapel-ID).

Syntax

Die Syntax dieses Befehls lautet wie folgt:

```
bcipost [batchID]
```

Parameter

batchID
Die Stapel-ID, die als Wert für den Parameter **BATCHID=** in der BCR-Datei angegeben wurde.

Beispiel

```
bcipost BCI200101140043
```

Befehl 'bcireport'

Der Befehl **bcireport** generiert die beiden Ausgabedateien 'bcioutput.*' und 'bcireport.*' (* steht für die Stapel-ID).

Die Datei 'bcioutput.*' enthält die Werte für den Schlüssel **PREID**, den Zertifikatstyp und die PKCS#7-Zeichenfolgen für alle Datensätze mit einer übereinstimmenden Stapel-ID.

In der Datei 'bcireport.*' ist der Status der Anforderung angegeben. Sie enthält eine Liste mit den aktuellen Werten für Abschnitt und Status jeder Zertifikatsanforderung, die mit der gegebenen Stapel-ID übereinstimmt. Diese Datei kann in jedem Abschnitt des Prozesses erstellt werden, sobald die Anfangsinformationen mit dem Befehl **bciin** aus der BCR-Datei gelesen wurden.

Syntax

Die Syntax dieses Befehls lautet wie folgt:

```
bcireport [batchID]
```

Parameter

batchID
Die Stapel-ID, die als Wert für den Parameter **BATCHID=** in der BCR-Datei angegeben wurde.

Beispiel

```
bcireport BCI200101140043
```

Befehl 'bcistart'

Der Befehl **bcistart** führt den gesamten BCI-Prozess vom Anfang bis zum Ende aus (**bciin**, **bcirun**, **bcipost**).

Syntax

Die Syntax dieses Befehls lautet wie folgt:

```
bcistart [batchID] [TPKI password]
```

Parameter

batchID
Die Stapel-ID, die als Wert für den Parameter **BATCHID=** in der BCR-Datei angegeben wurde.

TPKI password
Das TPKI-Kennwort ist das Steuerungskennwort für das Tivoli PKI-System.

Beispiel

```
bcirunstart BCI200101140043 adpass23
```

BCI-Ausgabedateien und -Protokolldateien

Alle BCI-Ausgabe- und Protokolldateien befinden sich in dem Verzeichnis 'usr/lpp/iau/pkrf/Domains/*xxxxDomäne*/logs'. Hierbei steht *xxxxDomäne* für den Tivoli PKI-Domänennamen. Der Administrator muss sicherstellen, dass in diesem Verzeichnis genügend Plattenspeicherplatz verfügbar ist. Die Ausgabe- und Protokolldateien werden nachfolgend beschrieben.

BCI-Ausgabedateien:

- bcireport.* (* steht für die Stapel-ID)
- bcioutput.* (* steht für die Stapel-ID)

BCI-Protokolldateien:

- bcistart.log.* (* steht für die Stapel-ID)
- bciin.log.* (* steht für den Namen der BCR-Datei)
- bcirunstart.log.* (* steht für die Stapel-ID. Diese Protokolldatei wird nur dann erstellt, wenn dieser Schritt separat vom BCI-Prozess ausgeführt wurde).
- bcirun.log.* (* steht für die Stapel-ID)
- bcipost.log.* (* steht für die Stapel-ID)

BCI-Zertifikatsverwaltung

Nachdem der BCI-Prozess abgeschlossen ist, werden die BCI-Zertifikate an die RA-Datenbank gesendet. Diese gesendeten BCI-Zertifikate können dann über den RA Desktop verwaltet werden. Sie können den Status der BCI-Zertifikate in jedem Abschnitt des BCI-Prozesses prüfen, indem Sie den Befehl **bcireport** ausführen. Die gesamten BCI-Anforderungsdaten werden in der Tabelle BCIRT der Datenbank PKRF auf dem RA-Server gespeichert. BCI enthält keine Tools, um Einträge in dieser Tabelle zu löschen.

Dienstprogramm CA Key Update

Mit dem Dienstprogramm CA Key Update können Sie eine Schlüsselaktualisierung - einen so genannten *Rollover-Prozess* - aus einem unbeschädigten CA-Schlüsselpaar auf das nächste CA-Schlüsselpaar einleiten. Sobald die Erstellung vorgenommen wurde, verwendet der CA beim Unterzeichnen von Zertifikaten das neue Schlüsselpaar. Der Administrator legt fest, ob das alte Schlüsselpaar versetzt oder gelöscht werden soll, sobald das neue Schlüsselpaar wirksam ist.

Wenn sich die Gültigkeitsdauer des CA-Schlüssels dem Ende zuneigt, sollte der Administrator einen Rollover-Prozess für das CA-Schlüsselpaar bei einem geplanten Systemabschluss des Tivoli PKI-Systems einplanen. Der Administrator sollte das System aus der Produktionsumgebung herausnehmen und alle notwendigen Vorbereitung dafür treffen, dass ausstehende Anforderungen erfüllt werden. Sobald das System beendet und heruntergefahren wurde, kann der Administrator das Dienstprogramm CA Key Update durch Absetzen des Befehls **cakeyroll** ausführen.

Hat der Administrator den Befehl **cakeyroll** abgesetzt, beginnt der erste Abschnitt des Rollover-Prozesses für den CA-Schlüssel. In diesem ersten Abschnitt wird ein neues CA-Schlüsselpaar erstellt. Mit dem neuen privaten Schlüssel werden drei Zertifikate erstellt. Jedes Zertifikat wird zur Prüfung von Zertifikaten verwendet, die mit dem alten privaten CA-Schlüssel unterzeichnet wurden, sowie von neuen Zertifikaten, die mit dem neuen privaten Schlüssel unterzeichnet wurden. Diese neuen Zertifikate sind im Directory unter dem Attribut ’caCertificate’ angegeben.Tabelle 17 veranschaulicht diesen Prozess.

Kunden können weiterhin die alten CA-Zertifikate mit öffentlichen Schlüsseln verwenden, bis sie eine Aktualisierung auf das neue CA-Zertifikat vornehmen. Das Zertifikat muss durch das neue CA-Zertifikat ersetzt werden, bevor der aktuelle Gültigkeitszeitraum des Zertifikats abläuft.

Tabelle 17. Rollover-Prozess für CA-Schlüssel

Zertifikat	Unterschriftsschlüssel	Gültigkeitsdatum (Anfang)	Gültigkeitsdatum (Ende)
newWithNew	Neu	Aktuelles Datum	Neues Verfallsdatum für den Schlüssel
newWithOld	Alt	Aktuelles Datum	Altes Verfallsdatum für den Schlüssel
oldWithNew	Neu	Altes Startdatum für den Schlüssel	Altes Verfallsdatum für den Schlüssel

Der zweite Teil des Rollover-Prozesses für den CA-Schlüssel beginnt, sobald die Verarbeitung des Befehls **cakeyroll** abgeschlossen ist. Der Befehl sollte die folgende Nachricht ausgeben.

```
CA-Key-Rollover wurde gestartet. Sie können nun den Befehl
Start_TA.sh eingeben.
```

Bitte versuchen Sie nicht, den Server in die Produktionsumgebung zu stellen oder durch das Absetzen von Anforderungen zu testen, nachdem Sie den Befehl **Start_TA.sh** abgesetzt haben. Diese Aktionen können Sie erst dann vornehmen, nachdem der Administrator geprüft hat, ob die CA-Protokolldatei die folgende Nachricht enthält:

```
Ausführung von CA-Key-Rollover für RA ra-name erfolgreich.
```

Anmerkung: Bei mehreren RAs muss für jede RA eine Nachricht in der Protokolldatei angegeben sein.

Sobald der Administrator festgestellt hat, dass die Nachrichten in der CA-Protokolldatei angegeben sind, kann er das Tivoli PKI-System in die Produktionsumgebung zurückstellen.

Die Prozeduren für die Aktualisierung des CA-Schlüssel sind unter „CA-Schlüssel aktualisieren” auf Seite 30 ausführlich beschrieben.

Nachdem der CA-Schlüssel-Rollover-Prozess abgeschlossen ist, muss der Administrator ermitteln, ob der CA als untergeordneter CA Teil einer Hierarchie war. Ist dies der Fall, muss der Administrator die Hierarchie mit den entsprechenden RAs wiederherstellen. Ausführliche Angaben zur Wiederherstellung der Hierarchie finden Sie unter „Aktualisierungen nach Änderung der CA-Hierarchie vornehmen” auf Seite 29.

Syntax

```
cakeyroll
```

Wenn der Befehl **cakeyroll** aufgerufen wird, fordert er von Ihnen das Kennwort für das Steuerprogramm an. Dieses Kennwort haben Sie bei der Ausführung von ’CfgPostInstall’ angegeben.

Felder für Prüfereignisse

Tabelle 18 erläutert die Informationen, die in Tivoli PKI-Prüfereignissen enthalten sind.

Tabelle 18. Felder für Prüfereignisse

Feldname	Beschreibung
Ereignisname	Die Ereigniskennung, die von einem Prüf-Client als Token angegeben wird.
Betroffene Entität	Die Entität, die von der Aktion betroffen ist, für die ein Prüfereignis gesendet wird. Diese Information wird von einem Prüf-Client angegeben.
Art der betroffenen Entität	Die Art der betroffenen Entität. Diese Information wird von einem Prüf-Client angegeben.
Berechtigte Entität	Diese Entität hat die Operation berechtigt. Diese Information wird von einem Prüf-Client angegeben.
Aufgabe der berechtigten Entität	Der Aufgabenbereich der berechtigten Entität.
Speichermedium	Sofern verfügbar, das für diese Operation angegebene Speichermedium. Diese Information wird von einem Prüf-Client angegeben.

Tabelle 18. Felder für Prüfereignisse (Forts.)

Feldname	Beschreibung
Bewertungsstufe	Die Bewertung des Ereignisses: entweder 'Information' oder 'Alert'.
Typ der berichtenden Komponente	Der Typ der Tivoli PKI-Komponente, die das Ereignis meldet.
Client-Quelle	Identifizierungsinformationen für die Tivoli PKI-Komponente, die das Ereignis sendet.
Client-Zeitmarke	Die Uhrzeit, an der das Prüfereignis von einer Tivoli PKI-Komponente gesendet wurde.
Zeitmarke	Die Uhrzeit, an der das Prüfereignis in die Datenbank oder in eine Datei geschrieben wurde.
Zusatzinformationen	Zusätzliche Informationen, die für die Operation relevant sind. Diese Informationen werden von einem Prüf-Client angegeben.

Prüfereignisse

Tabelle 19 erläutert die Tivoli PKI-Prüfereignisse und gibt an, ob ein Ereignis verbindlich oder optional ist.

Tabelle 19. Prüfereignisse

Ereignis	Beschreibung	Verbindlich oder optional
Schlüsselverwaltung		
KeyGeneration	Gibt an, dass ein Chiffrierschlüssel generiert wurde.	verbindlich
KeyImport	Gibt an, dass ein Chiffrierschlüssel in Tivoli PKI importiert wurde.	optional
KeyExport	Gibt an, dass ein Chiffrierschlüssel aus Tivoli PKI exportiert wurde.	optional
KeyStorage	Gibt an, dass ein Chiffrierschlüssel gespeichert wurde.	optional
KeyRollover	Gibt an, dass ein Chiffrierschlüssel durch einen neuen Schlüssel ersetzt wurde. Dieser Schlüssel wird für den gleichen Zweck eingesetzt wie der alte Schlüssel.	optional
KeyCompromise	Gibt an, dass ein Chiffrierschlüssel nicht mehr sicher ist.	verbindlich
CAKeyDistribution	Gibt an, dass der öffentliche Schlüssel des CA in das Directory geschrieben wurde.	verbindlich
Zertifikatsverwaltung		
CertGeneration	Gibt an, dass ein Zertifikat generiert wurde.	verbindlich
CertRevocation	Gibt an, dass ein Zertifikat widerrufen wurde.	verbindlich
CertRenewal	Gibt an, dass ein Zertifikat erneuert wurde.	verbindlich
CertSuspension	Gibt an, dass ein Zertifikat temporär ausgesetzt wurde.	verbindlich

Tabelle 19. Prüfereignisse (Forts.)

Ereignis	Beschreibung	Verbindlich oder optional
CertResumption	Gibt an, dass ein zuvor ausgesetztes Zertifikat aktiviert wurde.	verbindlich
CRLQuery	Gibt an, dass die Zertifikatswiderrufsliste (CRL) gelesen wurde.	optional
CRLUpdate	Gibt an, dass die Zertifikatswiderrufsliste (CRL) aktualisiert wurde.	verbindlich
SubmitCertRequest	Gibt an, dass eine Zertifikatsanforderung übergeben wurde.	optional
Enrollment	Gibt an, dass eine RA eine Registrierung bei einem CA angefordert hat.	verbindlich
Unenrollment	Gibt an, dass eine RA das Aufheben einer Registrierung bei einem CA angefordert hat.	verbindlich
CertDeletion	Gibt an, dass der CA ein Zertifikat aus der Zertifikatsdatenbank gelöscht hat.	optional
Sicherheitsrelevant		
SuccessfulAuthWithPassword	Gibt an, dass ein Authentifizierungsversuch mit Hilfe eines Kennworts erfolgreich war.	verbindlich
UnsuccessAuthWithPassword	Gibt an, dass ein Authentifizierungsversuch mit Hilfe eines Kennworts fehlgeschlagen ist.	verbindlich
SuccessfulAuthWithCert	Gibt an, dass ein Authentifizierungsversuch mit Hilfe eines Zertifikats erfolgreich war.	verbindlich
UnsuccessfulAuthWithCert	Gibt an, dass ein Authentifizierungsversuch mit Hilfe eines Zertifikats fehlgeschlagen ist.	verbindlich
SuccessfulCertValidation	Gibt an, dass die gesamte Zertifizierungskette bis hin zum Zertifikat des Stamm-CA geprüft wurde.	verbindlich
UnsuccessfulCertValidation	Gibt an, dass die gesamte Zertifizierungskette bis hin zum Zertifikat des Stamm-CA nicht bestätigt wurde.	verbindlich
PasswordChange	Gibt an, dass ein Kennwort erfolgreich geändert wurde.	verbindlich
ACLUpdate	Gibt an, dass ein Benutzer oder eine Entität der Zugriffssteuerungsliste (ACL) hinzugefügt oder aus der Liste gelöscht wurde.	verbindlich
SuccessfulIntegrityCheck	Gibt an, dass ein Versuch, die Integrität eines durch eine Transaktion mit einer Nicht-Tivoli PKI-Komponente entstandenen Protokolleintrag zu testen, erfolgreich war.	verbindlich
UnsuccessfulIntegrityCheck	Gibt an, dass ein Versuch, die Integrität eines durch eine Transaktion mit einer Nicht-Tivoli PKI-Komponente entstandenen Protokolleintrag zu testen, fehlgeschlagen ist.	verbindlich
SuccessfulAcquirePrivilege	Gibt an, dass die Anforderung eines bestimmten Zugriffs auf einen Tivoli PKI-KeyStore erfolgreich war.	verbindlich

Tabelle 19. Prüfereignisse (Forts.)

Ereignis	Beschreibung	Verbindlich oder optional
UnsuccessfulAcquirePrivilege	Gibt an, dass die Anforderung eines bestimmten Zugriffs auf einen Tivoli PKI-KeyStore fehlgeschlagen ist.	verbindlich
Aktionen des Sicherheitsbeauftragten		
SOAdd	Gibt an, dass dem System ein Prüfadministrator hinzugefügt wurde.	verbindlich
SODelete	Gibt an, dass ein Prüfadministrator vom System entfernt wurde.	verbindlich
AudEventMaskChange	Gibt an, dass die Maske geändert wurde, die die Gruppe von Prüfereignissen definiert, die ein Client an den Server senden kann.	verbindlich
CACrossCertRequest	Gibt an, dass ein Zertifikat eines gegenseitig zertifizierten CA angefordert wurde.	verbindlich
CAHierarchicalCertReq	Gibt an, dass ein Zertifikat eines hierarchisch zertifizierten CA angefordert wurde.	verbindlich
SubmitRevocationRequest	Gibt an, dass ein Registrator (RA-Administrator) eine Widerrufsanforderung übergeben hat.	optional
RequestSetRenewable	Gibt an, dass ein Registrator angefordert hat, ein Zertifikat mit dem Status 'erneuerbar' zu definieren.	verbindlich
RequestSetNonRenewable	Gibt an, dass ein Registrator angefordert hat, ein Zertifikat mit dem Status 'nicht erneuerbar' zu definieren.	verbindlich
RequestPend	Gibt an, dass ein Registrator angefordert hat, eine Identitätsnachweisanforderung in den Wartestatus zu setzen.	verbindlich
RA-Ereignisse		
ReceiptOfCertRequest	Gibt an, dass eine Zertifikatsanforderung von einer RA empfangen wurde.	optional
ReceiptOfRevocationRequest	Gibt an, dass eine Widerrufsanforderung für ein Zertifikat von einer RA empfangen wurde.	optional
ReceiptOfRenewalRequest	Gibt an, dass eine Erneuerungsanforderung für ein Zertifikat von einer RA empfangen wurde.	optional
RequestApproval	Gibt an, dass eine RA eine Zertifikatsanforderung bestätigt hat.	verbindlich
RequestRejection	Gibt an, dass eine RA eine Zertifikatsanforderung zurückgewiesen hat.	verbindlich
RequestCompletion	Gibt an, dass eine Zertifikatsanforderung abgeschlossen wurde.	optional
Preregistration	Gibt an, dass ein Registrator eine Anforderung zur Vorabregistrierung erhalten hat.	verbindlich

Prüfung von Datenbankdaten

Die Tivoli PKI-Prüfdatenbank verwendet ein Schema, das auf den Empfehlungen im Standard 'Public Key Cryptography for the Financial Services Industry' (X9.57) basiert. In diesem Abschnitt werden folgende Datenbanktabellen beschrieben.

Anmerkung: In diesem Abschnitt entsprechen die Feldnamen der Prüfsätze den Spaltennamen in den Datenbanktabellen.

- Schlüssel

  Dies ist eine Steuertabelle für private/geheime Schlüssel, die zum Unterzeichnen, Verschlüsseln und Erzeugen von Nachrichtenauthentifizierungscodes (MAC) verwendet werden.

- Ereignisbewertung (event_severities)

  Diese Tabelle beschreibt die Bewertung von Ereignissen.

- Ereignissteuerung (event_ctl)

  Diese Tabelle beschreibt alle prüfbaren Ereignisse.

- Quellen

  Diese Tabelle enthält eine Liste aller Ereignisquellen.

- Berechtigte Entitäten (auth_entities)

  Diese Tabelle enthält eine Liste aller berechtigten Entitäten.

- Betroffene Entitäten (afctd_entity_types)

  Diese Tabelle enthält eine Liste aller betroffenen Aufgabenbereiche.

- Berechtigte Aufgabenbereiche (auth_roles)

  Diese Tabelle enthält eine Liste aller Aufgabenbereiche für berechtigte Entitäten.

- Komponentenarten (component_types)

  Diese Tabelle enthält eine Liste aller Komponentenarten.

- Prüfprotokoll (audit_log)

  Dies ist die Haupttabelle für Einträge im Prüfprotokoll.

- Systemereignis

  Diese Tabelle enthält Informationen, die für das gesamte Prüfsystem gelten. Die Tabelle hat nur eine Zeile.

Schlüsseltabelle

Die Schlüsseltabelle enthält Informationen zu allen vom Prüfsystem verwendeten Chiffrierschlüsseln.

Tabelle 20. Felder in der Schlüsseltabelle

Feld	Beschreibung	Datentyp
key_id	Die eindeutige interne Schlüsselkennung.	smallint
alg_oid	Der dem Schlüssel zugeordnete Algorithmus.	varchar

Tabelle 20. Felder in der Schlüsseltabelle (Forts.)

Feld	Beschreibung	Datentyp
label	Der KeyStore-Kennsatz oder ein Token zur Lokalisierung des realen Schlüssels.	varchar
integrity	Dieses Feld dient der Aufrechterhaltung der Integrität des Datensatzes.	varchar für Bitdaten

Tabelle für Ereignisbewertung

Diese Tabelle enthält Informationen zur Bewertung von Ereignissen. Diese Tabelle ist schreibgeschützt und wird bei Installation und Konfiguration geladen.

Tabelle 21. Felder in der Tabelle für die Ereignisbewertung

Feld	Beschreibung	Datentyp
severity_id	Die eindeutige interne Kennung der Ereignisbewertung.	smallint
severity_desc	Die NLS-Zeichenfolge (NLS = National Language Support) für die Bewertung.	varchar

Tabelle zur Ereignissteuerung

Diese Tabelle enthält Informationen zu allen Ereignissen, die ein Prüf-Client an den Prüf-Server weiterleiten kann. Diese Tabelle ist schreibgeschützt und wird bei Installation und Konfiguration geladen.

Tabelle 22. Felder in der Tabelle für die Ereignissteuerung

Feld	Beschreibung	Datentyp
event_id	Die eindeutige Ereigniskennung.	smallint
event_desc	Eine sichtbare Beschreibung des Ereignisses. Dieses Feld kann zur Anzeige von Informationen verwendet werden.	varchar
event_key	Eine kurze eindeutige Zeichenfolge, die das Ereignis kennzeichnet und beschreibt. Dieses Feld wird von den Java-Ressourcenpaketen verwendet.	varchar
event_severity_id	Die Bewertungs-ID des Ereignisses. Dies ist der fremde Schlüssel, der auf die Tabelle 'event_severities' verweist.	smallint

Quellentabelle

Diese Tabelle enthält eine Liste aller Prüf-Clients. Ein Prüf-Client ist eine Tivoli PKI-Komponente, die Prüfereignisse erzeugt.

Tabelle 23. Felder in der Quellentabelle

Feld	Beschreibung	Datentyp
source_id	Die eindeutige Kennung des Prüf-Clients.	smallint
Quelle	Die Kennung des Prüf-Clients, die zur Anzeige genutzt werden kann. In der Regel handelt es sich hierbei um den DN des Prüf-Clients.	varchar
integrity	Dieses Feld dient der Aufrechterhaltung der Integrität des Datensatzes.	varchar für Bitdaten

Tabelle der berechtigten Entitäten

Diese Tabelle enthält eine Liste aller berechtigten Entitäten. Eine berechtigte Entität berechtigt die Operation, für die ein Prüfereignis erzeugt wurde.

Tabelle 24. Felder in der Tabelle berechtigter Entitäten

Feld	Beschreibung	Datentyp
auth_entity_id	Die eindeutige interne Kennung der berechtigten Entität.	smallint
auth_entity_desc	Die Kennung der berechtigten Entität, die zur Anzeige genutzt werden kann. In der Regel handelt es sich hierbei um den DN der berechtigten Entität.	varchar
integrity	Dieses Feld dient der Aufrechterhaltung der Integrität des Datensatzes.	varchar für Bitdaten

Tabelle der berechtigten Aufgabenbereiche

Diese Tabelle enthält Informationen zu den Aufgabenbereichen berechtigter Entitäten. Diese Tabelle ist schreibgeschützt und wird bei Installation und Konfiguration geladen.

Tabelle 25. Felder in der Tabelle berechtigter Aufgabenbereiche

Feld	Beschreibung	Datentyp
auth_role_id	Die eindeutige interne Kennung des berechtigten Aufgabenbereichs.	smallint
auth_role_desc	Die NLS-Zeichenfolge, die den berechtigten Aufgabenbereich beschreibt.	varchar

Tabelle der Arten betroffener Entitäten

Diese Tabelle enthält Informationen zu verschiedenen Arten betroffener Entitäten. Eine betroffene Entität wird von der Operation beeinflusst, für die ein Prüfereignis erzeugt wird. Diese Tabelle ist schreibgeschützt und wird bei Installation und Konfiguration geladen.

Tabelle 26. Felder in der Tabelle der Arten betroffener Entitäten

Feld	Beschreibung	Datentyp
afctd_entity_id	Die eindeutige interne Kennung der betroffenen Entität.	smallint
afctd_entity_desc	Die NLS-Zeichenfolge, die die betroffene Entität beschreibt.	varchar

Tabelle der Komponentenarten

Diese Tabelle enthält Informationen zu den verschiedenen Komponentenarten des Prüf-Clients. Diese Tabelle ist schreibgeschützt und wird bei Installation und Konfiguration geladen.

Tabelle 27. Felder in der Tabelle der Komponentenarten

Feld	Beschreibung	Datentyp
component_type_id	Die eindeutige interne Kennung der Komponentenart.	smallint
component_desc	Die NLS-Zeichenfolge, die die Komponentenart beschreibt.	varchar

Tabelle für Prüfprotokoll

Diese Tabelle enthält die Protokolleinträge.

Tabelle 28. Felder in der Prüfprotokolltabelle

Feld	Beschreibung	Datentyp
serial_num	Die eindeutige Seriennummer des Protokolleintrags.	smallint
src_date_time	Die Zeitmarke, die angibt, wann das Ereignis von der Quelle (Prüf-Client) erzeugt wurde.	Zeitmarke
cr_date_time	Die Zeitmarke, die angibt, wann der Protokolleintrag vom Prüf-Server erzeugt wurde.	Zeitmarke
event_id	Die interne Ereigniskennung. Dies ist ein fremder Schlüssel, der auf die Tabelle 'event_ctl' verweist.	smallint
source_id	Die interne Kennung der Quelle, die dieses Ereignis erzeugt hat. Dies ist ein fremder Schlüssel, der auf die Quellentabelle verweist.	smallint

Tabelle 28. Felder in der Prüfprotokolltabelle (Forts.)

Feld	Beschreibung	Datentyp
component_type_id	Die interne Kennung der Komponentenart der Quelle, die dieses Ereignis erzeugt hat. Dies ist ein fremder Schlüssel, der auf die Tabelle 'component_types' verweist.	smallint
auth_entity_id	Die interne Kennung der Entität, die dieses Ereignis berechtigt hat. Dies ist ein fremder Schlüssel, der auf die Tabelle 'auth_entities' verweist.	smallint
auth_role_id	Die interne Kennung des Aufgabenbereichs der Entität, die dieses Ereignis berechtigt hat. Dies ist ein fremder Schlüssel, der auf die Tabelle 'auth_entities' verweist.	smallint
afctd_entity	Der Name oder DN der Art der Entität, die von diesem Ereignis betroffen ist.	varchar
afctd_entity_id	Die interne Kennung der Art der Entität, die von diesem Ereignis betroffen ist.	smallint
storage_media	Das dem Prüfereignis zugeordnete Speichermedium.	varchar
extra_info	Dem Prüfereignis zugeordnete Zusatzinformationen.	varchar
sig_key_id	Die interne Kennung des Schlüssels, der zur Erzeugung des Integritätsfelds verwendet wurde. Dies ist ein fremder Schlüssel, der auf die Schlüsseltabelle verweist.	smallint
enc_key_id	Die interne Kennung des Schlüssels, der zur Verschlüsselung ausgewählter Felder des Datensatzes verwendet wird. Dies ist ein fremder Schlüssel, der auf die Schlüsseltabelle verweist. Im aktuellen Release von Tivoli PKI wird keines der Felder verschlüsselt.	smallint
integrity	Dieses Feld dient der Aufrechterhaltung der Integrität des Datensatzes.	varchar für Bitdaten

Systemtabelle

Diese Tabelle enthält Statusinformationen zur Prüfdatenbank.

Tabelle 29. Felder in der Systemtabelle

Feld	Beschreibung	Datentyp
first_sn	Die Seriennummer des ersten Protokolleintrag in audit_log.	integer
next_sn	Die Seriennummer des nächsten Protokolleintrags in audit_log.	integer
audit_int	Dieses Feld dient der Aufrechterhaltung der Integrität der Tabelle 'audit_log'.	varchar für Bitdaten
archive_int	Dieses Feld dient der Aufrechterhaltung der Integrität der Tabelle 'archive_ctl'.	varchar für Bitdaten
events_int	Dieses Feld dient der Aufrechterhaltung der Integrität der Tabelle 'events_ctl'.	varchar für Bitdaten
auth_ent_int	Dieses Feld dient der Aufrechterhaltung der Integrität der Tabelle 'auth_entities'.	varchar für Bitdaten
auth_role_int	Dieses Feld dient der Aufrechterhaltung der Integrität der Tabelle 'auth_roles'.	varchar für Bitdaten
sources_int	Dieses Feld dient der Aufrechterhaltung der Integrität der Quellentabelle.	varchar für Bitdaten
afctd_ent_type_int	Dieses Feld dient der Aufrechterhaltung der Integrität der Tabelle 'afctd_entities'.	varchar für Bitdaten
keys_int	Dieses Feld dient der Aufrechterhaltung der Integrität der Schlüsseltabelle.	varchar für Bitdaten
event_sevs_int	Dieses Feld dient der Aufrechterhaltung der Integrität der Tabelle der Ereignis-bewertung.	varchar für Bitdaten
comp_types_int	Dieses Feld dient der Aufrechterhaltung der Integrität der Tabelle der Komponententarten.	varchar für Bitdaten
system_int	Dieses Feld dient der Aufrechterhaltung der Integrität der Systemtabelle.	varchar für Bitdaten
sig_key_id	Die interne Kennung des Schlüssels, der zur Erzeugung der Integritätsfelder dieses Datensatzes verwendet wird. Dies ist ein fremder Schlüssel, der auf die Schlüsseltabelle verweist.	smallint

Fehlerbehebung

Bei der Standardinstallation von Tivoli PKI werden keine Protokolldateien für die ausführliche Stufe bzw. Debug-Stufe von Fehlernachrichten erstellt. Dieser Abschnitt beschreibt die Basisschritte zur Fehlerbehebung, wobei die Nachrichtenerstellung auf Debug-Stufe inaktiviert ist. Wenn Sie ausführlichere Informationen benötigen, können Sie die Debug-Nachrichtenerstellung mit Hilfe der unter „Fehlerbehebung mit aktivierter Nachrichtenerstellung auf Debug-Stufe" beschriebenen Prozedur aktivieren.

Grundlegende Fehlerbehebung

Befolgen Sie die nachfolgenden Anweisungen, um Probleme bei der Verwaltung von Tivoli PKI zu beheben:

1. Stoppen Sie das Tivoli PKI-System.
2. Starten Sie die Maschine erneut.
3. Starten Sie das Tivoli PKI-System.
4. Prüfen Sie den Status aller Komponenten, um den korrekten Betrieb zu gewährleisten.
5. Reproduzieren Sie das Problem, und prüfen Sie die Protokolle aller Komponenten, um den Fehler zu lokalisieren.

Fehlerbehebung mit aktivierter Nachrichtenerstellung auf Debug-Stufe

Wenn Sie bei einem Fehler ausführliche Unterstützung zur Fehlerbehebung benötigen, aktivieren Sie die Umgebungsvariable für die Debug-Stufe (DebugLevel). Sie können diesen Wert Ihren Bedürfnissen entsprechend anpassen, je nachdem, ob Sie mehr oder weniger Nachrichtendetails erhalten wollen. Die in dieser Variable angegebene Protokollstufe legt den Protokollumfang fest. Der Wert ist eine positive ganze Zahl im Bereich zwischen 0 und 1000. Je höher die Stufe, desto umfangreicher die Protokollierung. Die folgenden Tivoli PKI-Debug-Stufen werden empfohlen:

- **DebugLevel=25** - Minimale Protokollierung; es werden jedoch alle Fehler aufgezeichnet.

  Verwenden Sie diese Stufe für ständige Operationen, bei denen Probleme zwar nicht aktiv diagnostiziert werden, bei denen Sie die Protokolle jedoch gegebenenfalls einsehen wollen, falls doch etwas passiert.

- **DebugLevel=75** - Enthält zusätzlich die Protokollierung von darunter liegenden Softwareschichten.

  Verwenden Sie diese Stufe, wenn Probleme zwischen den CA- und RA-Servern auftreten. Das Ausgabevolumen ist etwa fünfmal höher als bei Debug-Stufe 25.

- **DebugLevel=101** - Enthält eine umfangreiche und detaillierte Protokollierung der höher stufigen RA-Server-Verarbeitung, einschließlich der Verarbeitung von Zertifikatsprofilen und der AFW-Interaktionen (Application Framework = Anwendungsgerüst).

  Verwenden Sie diese Stufe, wenn Sie versuchen, Probleme in den Schichten des RA-Servers für die Zertifikatsverarbeitung zu diagnostizieren. Das Ausgabevolumen ist etwa zehnmal höher als bei Debug-Stufe 25.

- **DebugLevel=201** - Umfangreiche Ablaufverfolgung (Tracing) kritischer, interner Funktionen, die sehr häufig verwendet werden.

  Verwenden Sie diese Stufe nur dann, wenn Sie versuchen, Probleme wie abnormale Beendigungen des RA-Servers zu diagnostizieren. Das Ausgabevolumen ist etwa hundertmal höher als bei Debug-Stufe 25.

Anmerkung: Aufgrund des hohen Protokollvolumens auf Stufe 100 darf diese Einstellung - sofern keine besonderen Umstände vorliegen - nicht in einer Produktionsumgebung verwendet werden. Auf dieser oder einer höheren Debug-Stufe besteht die Möglichkeit, dass der freie Speicherplatz im Dateisystem aufgebraucht wird, was zu zahlreichen Störungen im gesamten System führen kann.

So führen Sie die Fehlerbehebung mit aktivierter Nachrichtenerstellung auf Debug-Stufe aus (bei dieser Prozedur wird als Beispiel die Debug-Stufe 100 verwendet):

1. Stoppen Sie das Tivoli PKI-System.
2. Ändern Sie die Datei 'irgAutoCa.ini' folgendermaßen:
   - Unter AIX: Geben Sie für den Debug-Parameter in `/usr/lpp/iau/etc/TrustAuthority/irgAutoCa.ini` einen Wert zwischen 50 und 100 an.
   - Unter Windows NT: Geben Sie für den Debug-Parameter in `C:\Program Files\IBM\Trust Authority\etc\TrustAuthority\irgAutoCa.ini` einen Wert zwischen 50 und 100 an.
3. Aktivieren Sie folgendermaßen die Umgebungsvariable für die Debug-Stufe (DebugLevel):
   - Unter AIX: Geben Sie den folgenden Befehl in die Befehlszeile der Maschine ein, auf der sich der RA-Server befindet:
     ```
     export DebugLevel=
     ```
   - Unter Windows NT:
     a. Rufen Sie die Systemeigenschaften auf, indem Sie mit der rechten Maustaste auf das Symbol **Arbeitsplatz** im Windows NT Explorer klicken und **Eigenschaften** auswählen.
     b. Klicken Sie auf die Registerkarte **Umgebung**.
     c. Geben Sie **`DebugLevel`** in das Feld **Variable** und **`100`** in das Feld **Wert** ein.
     d. Klicken Sie auf **Setzen** und anschließend auf **Übernehmen**.
     e. Klicken Sie auf **OK**, um das Fenster mit den Systemeigenschaften zu schließen.
4. Starten Sie das Tivoli PKI-System.
5. Prüfen Sie den Status aller Komponenten, um den korrekten Betrieb zu gewährleisten.
6. Reproduzieren Sie das Problem, und prüfen Sie die Protokolle aller Komponenten, um den Fehler zu lokalisieren.

   Es werden Protokolldateien mit dem Dateinamen 'irgrasvr.log.*nnnn*' erstellt, wobei *nnnn* eine nach dem Zufallsprinzip generierte Zahl ist.
   - Unter AIX ist die Standardposition der Protokolldateien /usr/lpp/iau/etc/TrustAuthority/caSS.log.xxxxx.
   - Unter Windows NT ist die Standardposition c:\Program Files\IBM\Trust Authority\etc\TrustAuthority\caSS.log.xxxxx.

Glossar

In diesem Glossar werden alle Termini und Abkürzungen definiert, die in diesem Handbuch verwendet werden und die möglicherweise neu oder unbekannt und von Bedeutung sind.

Numerische Einträge

4758 PCI Cryptographic Coprocessor
Eine programmierbare, manipulationssensitive PCI-Bus-Verschlüsselungskarte, die die Ausführung von DES- und RSA-Verschlüsselungsoperationen mit hoher Geschwindigkeit ermöglicht. Die Verschlüsselungsprozesse werden in einem gesicherten und abgegrenzten Bereich auf der Karte ausgeführt. Die Karte entspricht den strengen Anforderungen des FIPS PUB 140-1 Level 4-Standards. In dem gesicherten und abgegrenzten Bereich kann Software ausgeführt werden. Der SET-Standard kann z. B. zur Verarbeitung von Kreditkartentransaktionen genutzt werden.

A

Abstract Syntax Notation One (ASN.1)
Eine ITU-Notation, die zum Definieren der Syntax von Informationsdaten benutzt wird. Sie definiert eine Reihe einfacher Datentypen und gibt eine Notation für die Identifizierung dieser Typen und die Angabe von Werten für diese Typen an. Diese Notationen können verwendet werden, wenn es erforderlich ist, die abstrakte Syntax von Informationen zu definieren, ohne damit die Art der Verschlüsselung dieser Informationen für die Übertragung zu beeinträchtigen.

ACL
Access Control List - Zugriffssteuerungsliste.

Aktionsprotokoll
Die Aufzeichnung aller Ereignisse, die während der gesamten Gültigkeitsdauer eines Identitätsnachweises aufgetreten sind.

American National Standard Code for Information Interchange (ASCII)
Der Standardcode, der für den Austausch von Informationen zwischen Datenverarbeitungssystemen, DFV-Systemen und zugehöriger Hardware verwendet wird. ASCII verwendet einen codierten Zeichensatz, der aus Zeichen von 7 Bit Länge (bzw. 8 Bit bei Paritätsprüfung) besteht. Der Zeichensatz besteht hierbei aus Steuerzeichen und Schriftzeichen.

American National Standards Institute (ANSI)
Eine Organisation, die die Verfahrensweisen definiert, mit deren Hilfe akkreditierte Organisationen freiwillig eingehaltene Industriestandards in den Vereinigten Staaten festlegen und verwalten. Ihr gehören Hersteller, Verbraucher und allgemeine Interessenvertretungen an.

Anforderungs-ID
Ein aus 24 bis 32 Zeichen bestehender ASCII-Wert, der zur eindeutigen Identifikation einer Zertifikatsanforderung gegenüber der RA dient. Dieser Wert kann bei der Transaktion für die Zertifikatsanforderung verwendet werden, um den Status der Anforderung oder des zugehörigen Zertifikats abzurufen.

ANSI
American National Standards Institute.

Applet
Ein in der Programmiersprache Java geschriebenes Computerprogramm, das innerhalb eines Java-kompatiblen Webbrowsers ausgeführt werden kann. Wird auch als Java-Applet bezeichnet.

Art
Siehe Objektart.

ASCII
American National Standard Code for Information Interchange.

ASN.1
Abstract Syntax Notation One.

Asymmetrische Verschlüsselung
Ein Verschlüsselungsverfahren, das zur Ver- und Entschlüsselung unterschiedliche, asymmetrische Schlüssel verwendet. Jedem Benutzer wird hierbei ein Schlüsselpaar zugeordnet, das einen allgemeinen, für alle zugänglichen Schlüssel und einen privaten Schlüssel umfasst, der nur dem jeweiligen Benutzer bekannt ist. Eine gesicherte Transaktion kann ausgeführt werden, wenn der öffentliche Schlüssel sowie der zugehörige private Schlüssel übereinstimmen. In diesem Fall kann die Transaktion entschlüsselt werden. Dieses Verfahren wird auch als Verschlüsselung auf der Basis von Schlüsselpaaren bezeichnet. *Gegensatz zu* Symmetrische Verschlüsselung.

Asynchrone Übertragung
Ein Übertragungsmodus, bei dem Sender und Empfänger nicht gleichzeitig vorhanden sein müssen.

Authentifizierung
Der Vorgang, bei dem die Identität eines Teilnehmers an einer Übertragung zuverlässig überprüft wird.

B

Base64-Verschlüsselung
Ein häufig verwendetes Verfahren bei der Übertragung von Binärdaten mit MIME.

Basic Encoding Rules (BER)
Die Regeln, die in ISO 8825 für die Verschlüsselung von in ASN.1 beschriebenen Dateneinheiten angegeben sind. Die Regeln geben das Verschlüsselungsverfahren, jedoch nicht die abstrakte Syntax an.

Benutzerauthentifizierung
Der Prozess, mit dem überprüft wird, ob der Absender einer Nachricht die berechtigte Person ist, als die er sich ausgibt. Der Prozess überprüft außerdem, ob ein Kommunikationsteilnehmer auch tatsächlich mit dem erwarteten Endbenutzer oder System in Verbindung steht.

BER
Basic Encoding Rules.

Berechtigung
Die Erlaubnis, auf eine Ressource zuzugreifen.

Bestreiten
Etwas als unwahr zurückweisen. Dies ist z. B. dann der Fall, wenn ein Benutzer abstreitet, eine bestimmte Nachricht gesendet oder eine bestimmte Anforderung übergeben zu haben.

Browser
Siehe Web-Browser.

Browser-Zertifikat
Ein digitales Zertifikat, das auch als Zertifikat der Client-Seite bezeichnet wird. Es wird von einem CA über einen für SSL aktivierten Web-Server ausgestellt. Die Schlüssel in einer verschlüsselten Datei ermöglichen dem Inhaber des Zertifikats das Verschlüsseln, Entschlüsseln und Unterzeichnen von Daten. Normalerweise werden diese Schlüssel im Web-Browser gespeichert. In bestimmten Anwendungen können die Schlüssel auf Smart-Cards oder anderen Speichermedien gespeichert werden. *Siehe auch* Digitales Zertifikat.

Bytecode
Maschinenunabhängiger Code, der mit dem Java-Compiler generiert und mit dem Java-Interpreter ausgeführt wird.

C

CA
Certificate Authority - Zertifikatsaussteller.

CA-Hierarchie
Bei Tivoli PKI eine Sicherungsstruktur, bei der ein CA auf der höchsten Ebene positioniert ist. Anschließend können bis zu vier weitere Ebenen mit untergeordneten CAs definiert werden. Wenn Benutzer oder Server bei einem

Zertifikatsaussteller registriert werden, wird ihnen ein von diesem Aussteller unterzeichnetes Zertifikat zugeordnet. Außerdem übernehmen sie die Zertifizierungshierarchie der übergeordneten Ebenen.

CA-Server
Der Server für die CA-Komponente von Tivoli PKI.

CAST-64
Ein Block-Cipher-Algorithmus, der mit einer Blockgröße von 64 Bit und einem 6-Bit-Schlüssel arbeitet. Er wurde von Carlisle Adams und Stafford Tavares entwickelt.

CA-Zertifikat
Ein Zertifikat, das vom Web-Browser eines Benutzers auf dessen Anforderung hin von einem nicht identifizierten CA akzeptiert wird. Der Browser kann dann dieses Zertifikat verwenden, um für die Kommunikation mit Servern, die über Zertifikate dieses CAs verfügen, eine Authentifizierung durchzuführen.

CCA
IBM Common Cryptographic Architecture.

CDSA
Common Data Security Architecture.

CGI
Common Gateway Interface.

Client
(1) Eine Funktionseinheit, die gemeinsam benutzte Services von einem Server empfängt. (2) Ein Computer oder Programm, der/das Services von einem anderen Computer oder Programm anfordert.

Client/Server
Ein Modell für die verteilte Verarbeitung, bei dem ein Programm an einem Standort eine Anforderung an ein Programm an einem anderen Standort sendet und auf eine Antwort wartet. Das anfordernde Programm wird als Client, das antwortende als Server bezeichnet.

Codeunterzeichnung
Ein Verfahren zum Unterzeichnen ausführbarer Programme mit einer digitalen Unterschrift. Die Codeunterzeichnung dient zur Verbesserung der Zuverlässigkeit von Softwarekomponenten, die über das Internet verteilt werden.

Common Cryptographic Architecture (CCA)
IBM Software, die einen konsistenten Verschlüsselungsansatz auf den wichtigsten IBM Computerplattformen bietet. Sie unterstützt Anwendungssoftware, die in einer Vielzahl von Programmiersprachen geschrieben wurde. Die Anwendungssoftware kann hierbei die CCA-Services aufrufen, um eine breite Palette kryptografischer Funktionen (einschließlich der DES- und der RSA-Verschlüsselung) auszuführen.

Common Data Security Architecture (CDSA)
Eine Initiative zum Definieren eines umfassenden Ansatzes für Sicherheitsservices und Sicherheitsverwaltungsoperationen bei computerbasierten Sicherheitsanwendungen. Diese Architektur wurde von Intel entworfen und dient dazu, Computerplattformen für Anwendungen sicherer zu gestalten.

Common Gateway Interface (CGI)
Ein Standardverfahren zum Übertragen von Informationen zwischen Web-Seiten und Webservern.

CRL
Certificate Revocation List - Zertifikatswiderrufsliste.

CRL-Publikationsintervall
Dieses Intervall wird in der CA-Konfigurationsdatei definiert und gibt das Zeitintervall zwischen zwei Publikationen der Zertifikatswiderrufsliste im Directory an.

D

Dämon

Ein Programm, das Tasks im Hintergrund ausführt. Es wird implizit aufgerufen, wenn eine Bedingung auftritt, die die Hilfe des Dämons erforderlich macht. Es ist nicht erforderlich, dass der Benutzer über die Ausführung des Dämons unterrichtet wird, da der Dämon normalerweise vom System automatisch gestartet wird. Ein Dämon kann über eine unbegrenzte Zeit hinweg ausgeführt oder vom System in bestimmten Zeitintervallen erneut generiert werden.

Der Terminus (englisch *demon*) stammt aus der Mythologie. Später wurde er aber als Akronym für den Ausdruck ″Disk And Execution MONitor″ (Platten- und Ausführungsüberwachungsprogramm) erklärt.

Data Encryption Standard (DES)

Eine Verschlüsselungs-Block-Cipher, die 1977 von der US-Regierung als offizieller Standard definiert und übernommen wurde. Dieser Standard wurde ursprünglich von IBM entwickelt. DES wurde seit seiner Veröffentlichung umfassend untersucht und stellt ein allgemein bekanntes und häufig verwendetes Verschlüsselungssystem zur Verfügung.

Bei DES handelt es sich um ein symmetrisches Verschlüsselungssystem. Um es für die Datenübertragung einzusetzen, müssen sowohl der Sender als auch der Empfänger den selben, geheimen Schlüssel kennen. Dieser Schlüssel wird zum Ver- und Entschlüsseln der Nachricht verwendet. DES kann außerdem zur Durchführung von Verschlüsselungsoperationen für einzelne Benutzer eingesetzt werden, z. B. zum Speichern von verschlüsselten Dateien auf einer Festplatte. DES arbeitet mit einer Blockgröße von 64 Bit und verwendet für die Verschlüsselung einen 56-Bit-Schlüssel. Ursprünglich wurde dieser Standard für die Hardwareimplementierung entwickelt. DES wird von NIST alle fünf Jahre erneut als offizieller Verschlüsselungsstandard der US-Regierung zertifiziert.

Datenspeicherbibliothek (DL)

Ein Modul, das den Zugriff auf permanente Datenspeicher mit Zertifikaten, CRLs, Schlüsseln, Regeln und anderen sicherheitsrelevanten Objekten ermöglicht.

DEK

Document Encryption Key = Dokumentverschlüsselungsschlüssel.

DER

Distinguished Encoding Rules.

DES

Data Encryption Standard.

Diffie-Hellman

Ein Verfahren zur Datenverschlüsselung, das auf der Verwendung eines gemeinsamen Schlüssels auf einem nicht gesicherten Medium basiert und nach seinen Erfindern (Whitfield Diffie und Martin Hellman) benannt wurde.

Digitales Zertifikat

Ein elektronischer Identitätsnachweis, der von einer zuverlässigen Stelle für eine Person oder Entität ausgestellt wird. Jedes Zertifikat ist mit dem privaten Schlüssel des CAs unterzeichnet. Es bürgt für die Identität einer Person, eines Unternehmens oder einer Organisation.

Abhängig vom Aufgabenbereich des CAs kann das Zertifikat die Berechtigung seines Inhabers bestätigen, e-Business-Transaktionen über das Internet auszuführen. In gewisser Weise hat ein digitales Zertifikat eine ähnliche Funktion wie ein Führerschein oder ein Meisterbrief. Es bestätigt, dass der Inhaber des entsprechenden privaten Schlüssels berechtigt ist, bestimmte e-Business-Aktivitäten auszuführen.

Ein Zertifikat enthält Informationen über die Entität, die von ihm zertifiziert wird, gibt an, ob es sich um eine Person, eine Maschine oder ein Computerprogramm handelt und enthält als Teil dieser Informationen den zertifizierten öffentlichen Schlüssel dieser Entität.

Digitale Unterschrift

Eine codierte Nachricht, die an Dokumente oder Daten angefügt wird, und die Identität des Absenders nachweist. Eine digitale Unterschrift gewährleistet ein höheres Maß an Sicherheit als eine physische Unterschrift, da es sich hierbei nicht lediglich um einen verschlüsselten Namen oder eine Reihe einfacher Identifikationscodes handelt. Eine digitale Unterschrift enthält eine verschlüsselte Zusammenfassung der unterzeichneten Nachricht. Durch das Anfügen einer digitalen Unterschrift an eine Nachricht lässt sich der Absender also zweifelsfrei feststellen. (Die Unterschrift kann nur mit Hilfe des Schlüssels des Absenders erstellt werden.) Außerdem ermöglicht sie die Absicherung des Inhalts der unterzeichneten Nachricht, da die verschlüsselte Nachrichtenzusammenfassung mit dem Nachrichteninhalt übereinstimmen muss. Andernfalls wird die Unterschrift nicht als gültig identifiziert. Eine digi-

tale Unterschrift kann also nicht von einer Nachricht kopiert und für eine andere Nachricht verwendet werden, da sonst die Zusammenfassung (Hash-Code) nicht übereinstimmen würde. Alle Änderungen an der unterzeichneten Nachricht führen automatisch zum Verlust der Gültigkeit der Unterschrift.

Digitale Zertifizierung
Siehe Zertifizierung.

Digital Signature Algorithm (DSA)
Ein auf öffentlichen Schlüsseln basierender Algorithmus, der zum Standard für digitale Unterschriften (Digital Signature Standard = DSS) gehört. Er kann nur für digitale Unterschriften, jedoch nicht für die Verschlüsselung verwendet werden.

Directory
Eine hierarchische Struktur, die als globales Repository für Informationen zur Datenkommunikation (wie beispielsweise E-Mail oder Austausch von verschlüsselten Daten) konzipiert ist. Im Directory werden bestimmte Elemente gespeichert, die für die PKI-Struktur (PKI = Public Key Infrastructure) unbedingt erforderlich sind. Hierzu gehören die folgenden Elemente: öffentliche Schlüssel, Zertifikate und Zertifikatswiderrufslisten (CRLs).
Die Daten im Directory sind hierarchisch in einer Baumstruktur organisiert, wobei die oberste Ebene der Baumstruktur das Root-Verzeichnis ist. Häufig stehen Organisationen einer höheren Ebene für einzelne Länder, Regierungen oder Unternehmen. Benutzer oder Einheiten werden im Allgemeinen als ″Blätter″ einer solchen Baumstruktur dargestellt. Diese Benutzer, Organisationen, Standorte, Länder und Einheiten haben jeweils ihren eigenen Eintrag. Jeder Eintrag besteht aus Attributen, denen verschiedene Typen zugewiesen sind. Diese enthalten Informationen zu den Objekten, für die der jeweilige Eintrag steht.
Jeder Eintrag im Directory ist mit einem zugeordneten registrierten Namen (DN = Distinguished Name) verbunden. Dieser ist eindeutig, wenn der Eintrag ein Attribut umfasst, das für das tatsächliche Objekt als eindeutig bekannt ist. Im folgenden DN-Beispiel wurde als Land (C = Country) US, als Unternehmen (O = Organization) IBM, als Unternehmenseinheit (OU = Organization Unit) Trust und als allgemeiner Name (CN = Common Name) der Wert CA1 angegeben.

```
C=US/O=IBM/OU=Trust/CN=CA1
```

Directory-Server
In Tivoli PKI das IBM Directory. Dieses Directory unterstützt die LDAP-Standards und verwendet DB2 als Basissystem.

Distinguished Encoding Rules (DER)
Durch DER werden bestimmte Einschränkungen für BER definiert. Mit DER kann genau ein bestimmter Verschlüsselungstyp aus den verfügbaren und auf der Basis der Verschlüsselungsregeln als zulässig definierten Typen ausgewählt werden. Hierdurch werden alle Senderoptionen eliminiert.

DL
Data Storage Library = Datenspeicherbibliothek.

DN
Distinguished Name - Registrierter Name.

Dokumentverschlüsselungsschlüssel (DEK)
Normalerweise ein symmetrischer Ver-/Entschlüsselungsschlüssel, z. B. DES.

Domäne
Siehe Sicherheitsdomäne *und* Registrierungsdomäne.

DSA
Digital Signature Algorithm.

E

e-Business
Das Durchführen geschäftlicher Transaktionen über Netze und Computer, z. B. der Kauf und Verkauf von Waren und Dienstleistungen sowie der Transfer von Zahlungsmitteln mit Hilfe der digitalen Kommunikation.

e-Commerce
Unternehmensübergreifende Transaktionen wie beispielsweise der Kauf und Verkauf von Waren und Dienstleistungen (zwischen Unternehmen und ihren Kunden, Lieferanten, Subunternehmen und anderen) über das Internet. E-Commerce stellt einen Kernbestandteil des e-Business dar.

Endentität
Der Gegenstand eines Zertifikats, bei dem es sich nicht um einen CA handelt.

Entschlüsseln
Den Verschlüsselungsprozess rückgängig machen.

Exemplar
Bei DB2 bezeichnet man als Exemplar eine logische Datenbankverwaltungsumgebung zum Speichern von Daten und Ausführen von Anwendungen. Es ermöglicht die Definition einer allgemeinen Gruppe von Konfigurationsparametern für verschiedene Datenbanken.

Extranet
Ein Netz, das auf dem Internet basiert und eine ähnliche Technologie einsetzt. Unternehmen beginnen momentan mit dem Einsatz des Web Publishings, elektronischen Handels und der Nachrichtenübertragung sowie der Verwendung von Groupware für verschiedene Gruppen von Kunden, Partnern und internen Mitarbeitern.

F

File Transfer Protocol (FTP)
Ein Client/Server-Protokoll im Internet, das zum Übertragen von Dateien zwischen Computern benutzt wird.

Firewall
Ein Gateway zwischen Netzen, der den Informationsfluss zwischen diesen einschränkt. Normalerweise dienen Firewalls dem Schutz interner Netze gegen die nicht berechtigte Verwendung durch externe Personen.

FTP
File Transfer Protocol.

G

Gateway
Eine Funktionseinheit, mit deren Hilfe nicht kompatible Netze oder Anwendungen Daten austauschen können.

Gegenseitige Zertifizierung
Ein Trust-Modell, bei dem ein CA für einen anderen CA ein Zertifikat ausstellt, das den öffentlichen Schlüssel enthält, der dem entsprechenden privaten Unterschriftsschlüssel zugeordnet ist. Ein gegenseitig zertifiziertes Zertifikat ermöglicht Client-Systemen oder Endentitäten in einer Verwaltungsdomäne die sichere Kommunikation mit Client-Systemen oder Endentitäten in einer anderen Domäne.

Gesicherte Computerbasis (TCB)
Die Software- und Hardwareelemente, die zur Umsetzung der Computersicherheitsregeln eines Unternehmens verwendet werden. Alle Elemente oder Teilelemente, die zur Implementierung der Sicherheitsregeln eingesetzt werden können, sind sicherheitsrelevant und Bestandteil der TCB. Bei der TCB handelt es sich um ein Objekt, das durch die Sicherheitsperipherie begrenzt wird. Die Mechanismen, die zur praktischen Umsetzung der Sicherheitsregeln eingesetzt werden, dürfen nicht umgangen werden können und müssen verhindern, dass Programme Zugriff auf Systemprivilegien erlangen können, für die sie nicht berechtigt sind.

H

Hierarchie
Die Organisation von Zertifikatsausstellern (CAs) innerhalb einer Trust-Kette. Diese beginnt mit einem selbst unterzeichnenden CA oder übergeordneten Root-CA, der sich an der höchsten Position befindet, und endet mit dem CA, der Zertifikate für Endbenutzer ausstellt.

Höchster CA
Der CA, der innerhalb der PKI-CA-Hierarchie die höchste Position einnimmt.

HTML
Hypertext Markup Language.

HTTP
Hypertext Transaction Protocol.

HTTP-Server
Ein Server, der die Web-gestützte Kommunikation mit Browsern und anderen Programmen im Netz steuert.

Hypertext
Textsegmente, die einzelne oder mehrere Wörter umfassen oder Bilder enthalten, auf die der Leser mit der Maus klicken kann, um ein anderes Dokument aufzurufen und anzuzeigen. Diese Textsegmente werden als Hyperlinks bezeichnet. Ruft der Leser diese anderen Dokumente auf, stellt er zu diesen eine Hyperlink-Verbindung her.

Hypertext Markup Language (HTML)
Eine Formatierungssprache für das Codieren von Web-Seiten. HTML basiert auf SGML (Standard Generalized Markup Language).

Hypertext Transaction Protocol (HTTP)
Ein Client/Server-Protokoll für das Internet, mit dem Hypertext-Dateien im Web übertragen werden.

I

ICL
Issued Certificate List - Liste der ausgestellten Zertifikate.

Identitätsnachweis
Vertrauliche Informationen, die verwendet werden, um beim Austausch von Daten während der Authentifizierung die eigene Identität zu belegen. In Network Computing-Umgebungen ist die am häufigsten verwendete Form des Identitätsnachweises ein Zertifikat, das von einem CA erstellt und unterzeichnet wurde.

IniEditor
Bei Tivoli PKI ein Tool, mit dem Konfigurationsdateien editiert werden können.

Integrität
Ein System schützt seine Datenintegrität, wenn es die Änderung dieser Daten durch nicht berechtigte Personen verhindert. (Im Gegensatz hierzu versteht man unter dem Schutz der Vertraulichkeit von Daten, wenn verhindert wird, dass diese unberechtigten Personen zugänglich gemacht werden.)

Integritätsprüfung
Die Prüfung der Protokolleinträge, die für Transaktionen mit externen Komponenten aufgezeichnet wurden.

International Standards Organization (ISO)
Eine internationale Organisation, die sich mit der Entwicklung und Veröffentlichung von Standards befasst.

International Telecommunication Union (ITU)
Eine internationale Organisation, in der Verwaltungs- und private Industriebereiche globale Datenfernübertragungsnetze und -services koordinieren. Bei der Veröffentlichung von Informationen zur Datenfernübertragungstechnologie sowie den entsprechenden Regelwerken und Standards nimmt sie eine führende Position ein.

Interne Struktur
Siehe Schema.

Internet
Ein weltweiter Verbund von Netzen, die die elektronische Verbindung zwischen Computern und die Kommunikation zwischen den Computern über Softwareeinrichtungen wie elektronische Post (E-Mail) oder Web-Browser ermöglichen. So sind beispielsweise die meisten Universitäten in ein Netz eingebunden, das seinerseits eine Verbindung zu anderen ähnlichen Netzen hat, die zusammen das Internet bilden.

Internet Engineering Task Force (IETF)
Eine Gruppe, die sich schwerpunktmäßig mit dem Entwickeln und Definieren von Protokollen für das Internet befasst. Sie repräsentiert eine internationale Gruppe von Netzdesignern, -bedienern, -herstellern und -forschern. Die Aufgabe der IETF ist die Entwicklung der Internet-Architektur sowie die Gewährleistung der reibungslosen Verwendung des Internets.

Intranet
Ein Netz innerhalb eines Unternehmens, das sich im Allgemeinen hinter Firewalls befindet. Es basiert auf dem Internet und setzt eine ähnliche Technologie ein. Vom technischen Standpunkt aus ist ein Intranet eine Erweiterung des Internets. Zu den in beiden Netzen benutzten Komponenten gehören z. B. HTML und HTTP.

IPSec
Ein von der IETF entwickelter IPS-Standard (IPS = Internet Protocol Security). IPSec ist ein Protokoll der Vermittlungsschicht, das entwickelt wurde, um Services für die Gewährleistung der Sicherheit bei der Verschlüsselung zur Verfügung zu stellen, die kombinierte Funktionen zur Authentifizierung, Sicherung der Integrität, Zugriffssteuerung und Wahrung der Vertraulichkeit flexibel unterstützen. Aufgrund seiner leistungsfähigen Funktionen bei der Authentifizierung wurde dieser Standard von vielen Lieferanten von VPN-Produkten als Protokoll zum Aufbau sicherer Punkt-zu-Punkt-Verbindungen im Internet übernommen.

ISO
International Standards Organization.

ITU
International Telecommunication Union.

J

Java
Von Sun Microsystems, Incorporated, entwickelte plattformunabhängige Computertechnologien, die für den Netzbetrieb optimiert sind. Die Java-Umgebung besteht aus dem Java-Betriebssystem (Java-OS), den virtuellen Maschinen für verschiedene Plattformen, der objektorientierten Java-Programmiersprache und einer Reihe von Klassenbibliotheken.

Java-Anwendung
Ein eigenständiges Programm, das in der Programmiersprache Java geschrieben ist. Es wird außerhalb eines Web-Browsers ausgeführt.

Java-Applet
Siehe Applet. *Gegensatz zu* Java-Anwendung.

Java-Klasse
Eine Einheit mit Java-Programmcode.

Java-Sprache
Eine von Sun Microsystems entwickelte Programmiersprache, die speziell für die Verwendung in Applet- und Agent-Anwendungen konzipiert wurde.

Java Virtual Machine (JVM)
Der Teil der Java-Laufzeitumgebung, der zum Interpretieren von Bytecodes eingesetzt wird.

K

KeyStore (Schlüsselspeicher)
Eine DL zum Speichern von Identitätsnachweisen für Tivoli PKI-Komponenten, z. B. Schlüssel und Zertifikate, in einem verschlüsselten Format.

Klartext
Nicht verschlüsselte Daten. *Synonym zu* unverschlüsselter Text.

Klasse

Beim objektorientierten Entwurf bzw. bei der objektorientierten Programmierung eine Gruppe von Objekten, die über eine gemeinsame Definition verfügen und aus diesem Grund mit denselben Merkmalen, Verarbeitungsoperationen und Funktionsweisen arbeiten.

Kryptographie

Bei der Sicherung von Computern die Prinzipien, Verfahren und Methoden zur Verschlüsselung von unverschlüsseltem und zur Entschlüsselung von verschlüsseltem Text.

L

LDAP

Lightweight Directory Access Protocol.

Lightweight Directory Access Protocol (LDAP)

Ein Protokoll, mit dem auf das Directory zugegriffen werden kann.

Liste der ausgestellten Zertifikate (ICL)

Eine vollständige Liste der ausgestellten Zertifikate sowie deren aktueller Status. Die Zertifikate sind anhand der Seriennummer und des Status indexiert. Diese Liste wird vom CA verwaltet und in der CA-Datenbank gespeichert.

M

MAC

Message Authentication Code - Nachrichtenauthentifizierungscode.

MD4

Eine Nachrichtenauszugs-Hash-Funktion auf 128-Bit-Basis, die von Ron Rivest entwickelt wurde. Ihre Geschwindigkeit übersteigt die von MD2 um ein Mehrfaches.

MD5

Eine unidirektionale Nachrichtenauszugs-Hash-Funktion, die von Ron Rivest entwickelt wurde. Sie stellt eine verbesserte Version von MD4 dar. MD5 verarbeitet Eingabetext in 512-Bit-Blöcken, die in 16 32-Bit-Unterblöcke aufgeteilt werden. Die Ausgabe des Algorithmus ist eine Gruppe von vier 32-Bit-Blöcken, die verkettet werden und so einen 128-Bit-Hash-Wert bilden. Diese Funktion wird ebenfalls zusammen mit MD2 in dem PEM-Protokollen verwendet.

MD2

Eine Nachrichtenauszugs-Hash-Funktion auf 128-Bit-Basis, die von Ron Rivest entwickelt wurde. Sie wird zusammen mit MD5 in den PEM-Protokollen verwendet.

Modulus

In dem auf öffentlichen Schlüsseln basierenden RSA-Verschlüsselungssystem das Produkt (n) aus zwei hohen Primzahlen: p und q. Die optimale Größe für einen RSA-Modulus hängt von den individuellen Sicherheitsanforderungen ab. Je größer der Modulus, desto höher die Sicherheit. Die momentan von den RSA Laboratories empfohlenen Schlüsselgrößen hängen vom geplanten Einsatz des Schlüssels ab. Hierbei werden 768 Bit für Schlüssel zum persönlichen Gebrauch, 1024 Bit für den Unternehmensbereich und 2048 Bit für extrem wertvolle Schlüssel wie z. B. CA-Schlüsselpaare angegeben. Ein 768-Bit-Schlüssel wird voraussichtlich bis mindestens zum Jahr 2004 sicher sein.

Multipurpose Internet Mail Extensions (MIME)

Eine frei verfügbare Gruppe von Spezifikationen, die den Austausch von Text in Sprachen mit unterschiedlichen Zeichensätzen ermöglicht. Diese Spezifikationen unterstützen auch den Austausch von Multimedia-E-Mail zwischen unterschiedlichen Computersystemen, die Internet-Mail-Standards verwenden. So können E-Mail-Nachrichten beispielsweise andere Zeichensätze als den US-ASCII-Satz sowie erweiterten Text, Bilder oder Tondaten enthalten.

N

Nachrichtenauszug
Eine irreversible Funktion, bei der auf der Basis einer Nachricht beliebiger Länge eine Datenmenge mit fester Länge generiert wird. Bei MD5 handelt es sich z. B. um einen Nachrichtenauszugsalgorithmus.

Nachrichtenauthentifizierungscode (MAC)
Ein geheimer Schlüssel, der von Sender und Empfänger gemeinsam benutzt wird. Der Sender authentifiziert sich und der Empfänger prüft die hierbei zur Verfügung gestellten Daten. Bei Tivoli PKI werden MAC-Schlüssel für CA- und Prüfkomponenten in den KeyStores gespeichert.

National Security Agency (NSA)
Die offizielle Sicherheitsbehörde der US-Regierung.

NIST
National Institute of Standards and Technology, früher NBS (National Bureau of Standards). Aufgabe dieses Instituts ist die Unterstützung offener Standards und der Interoperabilität in den verschiedenen Bereichen der Computerbranche.

NLS
National Language Support - Unterstützung in der Landessprache.

NSA
National Security Agency.

O

Objekt
Beim objektorientierten Design oder bei der objektorientierten Programmierung eine abstrakte Entität, die zur Abgrenzung bestimmter Daten und der zugehörigen Operationen dient. *Siehe auch* Klasse.

Objektart
Die Art von Objekt, die im Directory gespeichert werden kann. Beispiele sind eine Firma, ein Konferenzraum, eine Einheit, eine Person, ein Programm oder ein Prozess.

Objekt-ID (OID)
Ein von einer Verwaltungsfunktion zugeordneter Datenwert, der den in ASN.1 definierten Typ aufweist.

ODBC
Open Database Connectivity.

Öffentlicher Schlüssel
In einem Paar aus einem öffentlichen und einem privaten Schlüssel steht dieser Schlüssel anderen Benutzern zur Verfügung. Er ermöglicht diesen Benutzern die Weiterleitung einer Transaktion an den Eigner des Schlüssels sowie die Prüfung einer digitalen Unterschrift. Mit einem öffentlichen Schlüssel verschlüsselte Daten können nur mit dem entsprechenden privaten Schlüssel entschlüsselt werden. *Gegensatz zu* Privater Schlüssel. *Siehe auch* Schlüsselpaar aus öffentlichem und privatem Schlüssel.

Open Database Connectivity (ODBC)
Ein Standard für den Zugriff auf unterschiedliche Datenbanksysteme.

Open Systems Interconnect (OSI)
Der Name der von ISO genehmigten Computernetzstandards.

OSI
Open Systems Interconnect.

P

PC-Karte
Eine mit einer Smart-Card vergleichbare Einheit, die auch als PCMCIA-Karte bezeichnet wird. Sie ist etwas größer als eine Smart-Card und verfügt im Allgemeinen über eine höhere Kapazität.

PEM
Privacy-Enhanced Mail.

PKCS
Public Key Cryptography Standards.

PKCS #1
Siehe Public Key Cryptography Standards.

PKCS #7
Siehe Public Key Cryptography Standards.

PKCS #10
Siehe Public Key Cryptography Standards.

PKCS #11
Siehe Public Key Cryptography Standards.

PKCS #12
Siehe Public Key Cryptography Standards.

PKI
Public Key Infrastructure.

PKIX
PKI auf X.509v3-Basis.

PKIX Certificate Management Protocol (PKIX CMP)
Ein Protokoll, das Verbindungen mit PKIX-kompatiblen Anwendungen ermöglicht. PKIX CMP verwendet als primäres Transportverfahren TCP/IP, es ist jedoch eine Abstraktionsebene oberhalb der Sockets-Schicht vorhanden. Dies ermöglicht die Unterstützung für zusätzliche Datenübertragungsoperationen mit Sendeaufrufen (Polling).

PKIX CMP
PKIX Certificate Management Protocol.

PKIX-Empfangseinheit
Der öffentliche HTTP-Server, der von einer bestimmten Registrierungsdomäne verwendet wird, um Anforderungen der Client-Anwendung von Tivoli PKI zu empfangen.

Privacy-Enhanced Mail (PEM)
Der vom Internet Architect Board (IAB) genehmigte Internet-Standard für die verbesserte Wahrung der Vertraulichkeit, der die sichere Übertragung elektronischer Post (E-Mail) über das Internet ermöglicht. Die PEM-Protokolle regeln Verschlüsselung, Authentifizierung, Nachrichtenintegrität und Schlüsselverwaltung.

Privater Schlüssel
In einem Paar aus einem öffentlichen und einem privaten Schlüssel steht dieser Schlüssel nur für seinen Eigner zur Verfügung. Er ermöglicht dem Eigner das Empfangen einer privaten Transaktion oder eine digitale Unterschrift. Die mit einem privaten Schlüssel unterzeichneten Daten können nur mit dem entsprechenden öffentlichen Schlüssel geprüft werden. *Gegensatz zu* öffentlicher Schlüssel. *Siehe auch* Schlüsselpaar aus öffentlichem und privatem Schlüssel.

Protokoll
Eine vereinbarte Konvention für die Kommunikation zwischen Computern.

Protokollierungssubsystem
Bei Tivoli PKI ein Subsystem, das die Unterstützungsfunktionen zum Protokollieren von sicherheitsrelevanten Aktionen bereitstellt. Es entspricht den Empfehlungen, die im X9.57-Standard unter *Public Key Cryptography for the Financial Services Industry* definiert wurden.

Proxy-Server
Eine Einheit, die zwischen einem Computer, der eine Zugriffsanforderung absetzt (Computer A) und einem Computer, auf den zugegriffen werden soll (Computer B), implementiert ist. Wenn ein Endbenutzer eine Anforderung für eine Ressource über Computer A absetzt, wird diese an den Proxy-Server geleitet. Dieser sendet die Anforde-

rung an Computer B, erhält von diesem die Antwort und leitet diese an den Endbenutzer weiter. Mit Hilfe eines Proxy-Servers kann über einen Computer, der sich innerhalb einer Firewall befindet, auf das World Wide Web zugegriffen werden.

Prüf-Client
Jeder Client im System, der Prüfereignisse an den Tivoli PKI-Prüf-Server sendet. Bevor ein Prüf-Client ein Ereignis an den Prüf-Server sendet, stellt er eine Verbindung zu diesem her. Nach der Herstellung der Verbindung verwendet der Client die Client-Bibliothek des Prüfsubsystems, um Ereignisse an den Prüf-Server zu übertragen.

Prüfprotokoll
Daten in Form eines logischen Pfades, die eine Folge von Ereignissen verbinden. Mit dem Prüfprotokoll können Transaktionen oder der bisherige Verlauf einer bestimmten Aktivität verfolgt werden.

Prüfprotokoll
Bei Tivoli PKI eine Tabelle in einer Datenbank, in der für jedes Prüfereignis ein Datensatz gespeichert wird.

Prüf-Server
Ein Tivoli PKI-Server, der zum Empfangen von Prüfereignissen von Prüf-Clients und zum Aufzeichnen dieser Ereignis in einem Prüfprotokoll dient.

Prüfzeichenfolge
Eine Zeichenfolge, die von einem Server oder einer Anwendung gesendet wird und zum Anfordern der Benutzerberechtigung dient. Der Benutzer, der zur Authentifizierung aufgefordert wird, unterzeichnet die Prüfzeichenfolge mit einem privaten Schlüssel. Der öffentliche Schlüssel des Benutzers sowie die unterzeichnete Prüfzeichenfolge werden zurück an den Server oder die Anwendung gesendet, der bzw. die die Authentifizierung anforderte. Der Server versucht anschließend, die unterzeichnete Prüfzeichenfolge mit Hilfe des öffentlichen Schlüssels des Benutzers zu entschlüsseln. Wenn die entschlüsselte Prüfzeichenfolge mit der ursprünglich gesendeten Prüfzeichenfolge übereinstimmt, gilt der Benutzer als authentifiziert.

Public Key Cryptography Standards (PKCS)
Informelle, herstellerübergreifende Standards, die im Jahr 1991 von den RSA Laboratories in Zusammenarbeit mit Repräsentanten verschiedener Computerhersteller entwickelt wurden. Diese Standards umfassen die RSA-Verschlüsselung, die Diffie-Hellman-Vereinbarung, die kennwortbasierte Verschlüsselung sowie die Syntax für erweiterte Zertifikate, verschlüsselte Nachrichten, Daten zu privaten Schlüsseln und für die Zertifizierung.

- PKCS #1 beschreibt ein Verfahren zum Verschlüsseln von Daten mit Hilfe des RSA-Verschlüsselungssystems auf der Basis öffentlicher Schlüssel. Er dient zur Erstellung digitaler Unterschriften und Briefumschläge.
- PKCS #7 definiert ein allgemeines Format für verschlüsselte Nachrichten.
- PKCS #10 definiert eine Standardsyntax für Zertifizierungsanforderungen.
- PKCS #11 definiert eine Programmierschnittstelle für Verschlüsselungseinheiten, z. B. Smart-Cards, die unabhängig vom verwendeten technologischen Konzept ist.
- PKCS #12 definiert ein portierbares Format zum Speichern oder Transportieren der privaten Schlüssel, Zertifikate und sonstiger geheimer Daten etc. eines Benutzers.

Public Key Infrastructure (PKI)
Ein Standard für Sicherheitssoftware, der auf der Verschlüsselung mit Hilfe öffentlicher Schlüssel basiert. Bei PKI handelt es sich um ein System digitaler Zertifikate, Zertifikatsaussteller, Registrierungsstellen, Zertifikatverwaltungsservices und verteilter Verzeichnisservices. Er dient zum Prüfen der Identität und Berechtigung aller Parteien, die an Transaktionen beteiligt sind, die über das Internet ausgeführt werden. Diese Transaktionen umfassen möglicherweise Operationen, zu deren Ausführung eine Identitätsprüfung erforderlich ist. Sie dienen z. B. zur Bestätigung des Ursprungs von Senderechtanforderungen, E-Mail-Nachrichten oder Finanztransaktionen.
PKI stellt öffentliche Chiffrierschlüssel und Benutzerzertifikate für die Authentifizierung durch eine berechtigte Einzelperson oder ein berechtigtes Unternehmen zur Verfügung. Er stellt Online-Verzeichnisse bereit, die die öffentlichen Chiffrierschlüssel und Zertifikate enthalten, die zur Überprüfung der digitalen Zertifikate, Identitätsnachweise sowie der digitalen Unterschriften verwendet werden.
PKI stellt außerdem Funktionen zur schnellen und effizienten Antwort auf Prüfabfragen und Anforderungen für öffentliche Chiffrierschlüssel bereit. Der Standard dient darüber hinaus zur Identifizierung potenzieller Sicherheitslücken im System und zur Verwaltung von Ressourcen zur Bearbeitung von Sicherheitsverletzungen. PKI bietet außerdem einen digitalen Zeitmarkenservice für wichtige Unternehmenstransaktionen.

R

RA

Registration Authority - Registrierungsstelle.

RA Desktop

Ein Java-Applet, das den RAs eine Grafikschnittstelle für die Verarbeitung von Anforderungen für Identitätsnachweise und zur Verwaltung dieser Nachweise während ihrer Gültigkeitsdauer zur Verfügung stellt.

RA-Server

Der Server für die RA-Komponente von Tivoli PKI.

RC2

Eine variable Schlüsselgrößen-Block-Cipher, die von Ron Rivest für RSA Data Security entwickelt wurde. *RC* steht für *Ron's Code* oder *Rivest's Cipher*. Sie arbeitet schneller als DES und löst diese Block-Cipher ab. Durch die Verwendung geeigneter Schlüsselgrößen kann sie in Bezug auf eine ausgedehnte Schlüsselsuche flexibler als DES gestaltet werden. Sie verfügt über eine Blockgröße von 64 Bit und arbeitet auf Softwareebene zwei- bis dreimal schneller als DES. RC2 kann in denselben Modi eingesetzt werden wie DES.
Durch eine Vereinbarung zwischen SPA (Software Publishers Association) und der US-Regierung nimmt RC2 einen speziellen Status ein. Hierdurch ist das Genehmigungsverfahren für den Export einfacher und schneller, als dies bei anderen Verschlüsselungsprodukten der Fall ist. Um die Voraussetzungen für eine rasche Exportgenehmigung zu erfüllen, muss ein Produkt mit einigen Ausnahmen die RC2-Schlüsselgröße auf 40 Bit beschränken. Eine zusätzliche Zeichenfolge kann verwendet werden, um Nichtberechtigte abzuwehren, die versuchen, eine umfangreiche Tabelle möglicher Verschlüsselungsvarianten vorauszuberechnen.

Regel-Exit

In einer Registrierungseinrichtung ein auf Unternehmensebene definiertes Programm, das von der Registrierungsanwendung aufgerufen wird. Die Regeln eines Regel-Exits implementieren die Unternehmens- und Sicherheitsbenutzervorgaben eines Unternehmens für den Registrierungsprozess.

Registrierter Name (DN)

Der eindeutige Name eines im Directory gespeicherten Dateneintrags. Der DN dient zur eindeutigen Identifizierung der Position eines Eintrags in der hierarchischen Struktur des Directory.

Registrierung

Bei Tivoli PKI das Abrufen von Identitätsnachweisen für die Verwendung über das Internet. Bei der Registrierung werden Zertifikate angefordert, erneuert und widerrufen.

Registrierungsattribut

Eine Registrierungsvariable, die in einem Registrierungsformular enthalten ist. Ihr Wert gibt die Informationen wider, die während der Registrierung erfasst werden. Der Wert des Registrierungsattributs bleibt während der gesamten Gültigkeitsdauer des Identitätsnachweises gleich.

Registrator

Ein Benutzer, der für den Zugriff auf RA Desktop sowie zur Verwaltung und Anforderung von Zertifikaten berechtigt ist.

Registrierungsstelle (RA)

Die Software, die zur Verwaltung digitaler Zertifikate verwendet wird und sicherstellt, dass die Unternehmensregeln vom ersten Empfang einer Registrierungsanforderung bis zum Zertifikatswiderruf angewendet werden.

Registrierungsdatenbank

Diese Datenbank enthält Informationen zu Zertifikatsanforderungen und ausgestellten Zertifikaten. In der Datenbank werden Registrierungsdaten gespeichert und alle Änderungen aufgezeichnet, die während der Gültigkeitsdauer an einem Zertifikat vorgenommen werden. Die Datenbank kann durch RA-Prozesse und Regel-Exits oder durch den Registrator aktualisiert werden.

Registrierungsdomäne

Eine Gruppe von Ressourcen, Regeln und Konfigurationsoptionen, die sich auf bestimmte Registrierungsprozesse für Zertifikate beziehen. Der Domänenname stellt einen untergeordneten Wert zur URL-Adresse dar, die zur Ausführung der Registrierungseinrichtung eingesetzt wird.

Registrierungseinrichtung
Ein Tivoli PKI-Anwendungsgerüst, das spezielle Verfahren zur Registrierung von Entitäten (z. B. Browser, Router, E-Mail-Einheiten und sichere Client-Anwendungen) und zur Verwaltung von Zertifikaten während ihrer Gültigkeitsdauer bereitstellt.

Registrierungsprozess
Bei Tivoli PKI die Schritte, die zur Überprüfung eines Benutzers ausgeführt werden. Durch den Registrierungsprozess werden Benutzer sowie deren öffentliche Schlüssel zertifiziert, um sie zur Teilnahme an den gewünschten Transaktionen zu berechtigen. Er kann lokal oder Web-gestützt, automatisch oder von einer tatsächlich mit Personen besetzten Registrierungsstelle ausgeführt werden.

Registrierungsvariable
Siehe Registrierungsattribut.

RSA
Ein auf öffentlichen Schlüsseln basierender Verschlüsselungsalgorithmus, der nach seinen Erfindern (Rivest, Shamir und Adelman) benannt wurde. Er wird zur Verschlüsselung und für digitale Unterschriften verwendet.

S

Schema
Beim Directory die interne Struktur, die zur Definition der Beziehungen zwischen den verschiedenen Objektarten verwendet wird.

Schlüssel
Bei der Verschlüsselung ein Wert, der zum Ver- und Entschlüsseln von Informationen verwendet wird.

Schlüsselpaar
Zusammengehörende Schlüssel, die bei der asymmetrischen Verschlüsselung eingesetzt werden. Ein Schlüssel wird zur Verschlüsselung, der andere zur Entschlüsselung verwendet.

Schlüsselpaar aus öffentlichem und privatem Schlüssel
Ein Schlüsselpaar aus öffentlichem und privatem Schlüssel stellt ein grundlegendes Element der Verschlüsselung auf der Basis von Schlüsselpaaren dar. (Diese Form der Verschlüsselung wurde im Jahr 1976 von Whitfield Diffie und Martin Hellman eingeführt, um Probleme bei der Schlüsselverwaltung zu lösen.) Nach diesem Konzept erhält jeder Benutzer ein Schlüsselpaar, bei dem einer als öffentlicher und einer als privater Schlüssel bezeichnet wird. Der öffentliche Schlüssel ist hierbei allgemein bekannt, der private Schlüssel wird hingegen geheim gehalten. Sender und Empfänger müssen geheime Daten nicht gemeinsam benutzen. Alle Kommunikationsoperationen werden lediglich auf der Basis öffentlicher Schlüssel ausgeführt. Die privaten Schlüssel werden niemals übertragen oder gemeinsam verwendet. Auf diese Weise ist es nicht mehr notwendig, sich auf die Sicherheit eines Übertragungskanals gegenüber Manipulationen zu verlassen. Die einzige Anforderung ist, dass öffentliche Schlüssel den entsprechenden Benutzern in einer gesicherten (authentifizierten) Weise (z. B. in einem gesicherten Verzeichnis) zugeordnet werden. Jeder Benutzer kann nun mit Hilfe dieser öffentlichen Daten eine vertrauliche Nachricht senden. Diese Nachricht kann nur mit einem privaten Schlüssel entschlüsselt werden, auf den allein der gewünschte Empfänger zugreifen kann. Darüber hinaus kann die Verschlüsselung auf der Basis von Schlüsselpaaren nicht nur zur Gewährleistung der Vertraulichkeit (Verschlüsselung), sondern auch für die Authentifizierung (digitale Unterschriften) eingesetzt werden.

Schlüsselsicherung und -wiederherstellung
Diese Funktion von Tivoli PKI ermöglicht das Sichern und Wiederherstellen von Endentitätszertifikaten und der zugehörigen, von Tivoli PKI zertifizierten öffentlichen und privaten Schlüssel. Die Zertifikate und Schlüssel werden in einer PKCS #12-Datei gespeichert. Diese Datei ist kennwortgeschützt. Das Kennwort wird beim Sichern des Zertifikats und der Schlüssel gesetzt.

Secure Electronic Transaction (SET)
Ein Branchenstandard für die Durchführung sicherer Kredit- oder Kundenkartenzahlungen über nicht gesicherte Netze. Der Standard formuliert Definitionen für die Authentifizierung von Kartenhaltern, Händlern sowie der Banken, durch die die Karten ausgestellt werden, da er die Ausstellung von Zertifikaten anfordert.

Secure Sockets Layer (SSL)
Ein IETF-Standardübertragungsprotokoll mit integrierten Sicherheitsservices, die für den Endbenutzer möglichst transparent sind. Es stellt einen digitalen, sicheren Kommunikationskanal zur Verfügung.

Ein SSL-fähiger Server empfängt SSL-Verbindungsanforderungen im Allgemeinen an einem anderen Anschluss (Port) als normale HTTP-Anforderungen. SSL erstellt eine Sitzung, in der die Austauschsignale zum Herstellen der Kommunikation zwischen zwei Modems nur einmal gesendet werden müssen. Anschließend wird die Kommunikation verschlüsselt und die Nachrichtenintegrität wird solange überprüft, bis die SSL-Sitzung abgelaufen ist.

Server

(1) In einem Netz eine Datenstation, die anderen Stationen Funktionen zur Verfügung stellt, wie beispielsweise ein Datei-Server. (2) In TCP/IP ein System in einem Netz, das die Anforderungen eines Systems an einem anderen Standort verarbeitet. Dieses Konzept wird als Client/Server-Modell bezeichnet.

Server-Zertifikat

Ein digitales Zertifikat, das von einem CA ausgegeben wird und es einem Web-Server ermöglicht, SSL-gestützte Transaktionen auszuführen. Wenn ein Browser über das SSL-Protokoll eine Verbindung zum Server herstellt, sendet der Server seinen öffentlichen Schlüssel an den Browser. Hierdurch kann die Identität des Servers authentifiziert werden und es können verschlüsselte Daten an den Server gesendet werden. *Siehe auch* CA-Zertifikat, Digitales Zertifikat *und* Browserzertifikat.

Servlet

Ein Server-Programm, das zusätzliche Funktionen für Server zur Verfügung stellt, die Java unterstützen.

SET

Secure Electronic Transaction.

SGML

Standard Generalized Markup Language.

SHA-1 (Secure Hash Algorithm)

Ein von NIST und NSA entwickelter Algorithmus, der beim DSS (Digital Signature Standard) verwendet wird. Der Standard wird als Secure Hash Standard bezeichnet; SHA ist der Algorithmus, der von diesem Standard verwendet wird. Er generiert einen 160-Bit-Hash-Code.

Sicherheitsdomäne

Eine Gruppe (z. B. Unternehmen, Arbeitsgruppe, Projektteam), deren Zertifikate vom gleichen CA zertifiziert wurden. Benutzer, die über ein von einem CA unterzeichnetes Zertifikat verfügen, können der Identität eines anderen Benutzers vertrauen, der ein Zertifikat besitzt, das vom selben CA unterzeichnet worden ist.

Sicherungsmodell

Eine Organisationskonvention, die regelt, wie Zertifikatsaussteller (CAs) andere Zertifikatsaussteller zertifizieren können.

Simple Mail Transfer Protocol (SMTP)

Ein Protokoll, mit dem elektronische Post über das Internet übertragen wird.

Site-Zertifikat

Dieser Zertifikatstyp ist mit einem CA-Zertifikat vergleichbar, gilt jedoch nur für eine bestimmte Website. *Siehe auch* CA-Zertifikat.

Smart-Card

Eine Hardwarekomponente, normalerweise in der Größe einer Kreditkarte, auf der die digitalen Schlüssel eines Benutzers gespeichert werden können. Eine Smart-Card kann kennwortgeschützt werden.

S/MIME

Ein Standard, der das Unterzeichnen und Verschlüsseln von elektronischer Post (E-Mail) unterstützt, die über das Internet übertragen wird. *Siehe* MIME.

SMTP

Simple Mail Transfer Protocol.

SSL

Secure Sockets Layer.

Standard Generalized Markup Language (SGML)

Ein Standard zur Beschreibung von Formatierungssprachen. HTML basiert auf SGML.

Symmetrischer Schlüssel
Ein Schlüssel, der sowohl für die Verschlüsselung als auch für die Entschlüsselung verwendet werden kann. *Siehe auch* Symmetrische Verschlüsselung.

Symmetrische Verschlüsselung
Eine Form der Verschlüsselung, bei der sowohl für die Ver- als auch für die Entschlüsselung derselbe Schlüssel verwendet wird. Die Sicherheit dieses Verfahren basiert auf dem Schlüssel. Wird dieser öffentlich bekannt gegeben, können die mit ihm bearbeiteten Nachrichten von jedem Benutzer ver- und entschlüsselt werden. Der Inhalt der übertragenen Daten kann nur dann geheim gehalten werden, wenn der Schlüssel nur den jeweils berechtigten Personen bekannt ist. *Gegensatz zu* Asymmetrische Verschlüsselung.

T

TCP/IP
Transmission Control Protocol/Internet Protocol.

TP
Trust Policy = Sicherungsregel.

Transaktions-ID
Eine Kennung, die die RA als Antwort auf eine Anforderung für eine Vorabregistrierung zur Verfügung stellt. Mit dieser ID kann ein Benutzer, der die Client-Anwendung von Tivoli PKI ausführt, ein vorab genehmigtes Zertifikat erhalten.

Transmission Control Protocol/Internet Protocol (TCP/IP)
Eine Gruppe von Übertragungsprotokollen, die Peer-zu-Peer-Konnektivitätsfunktionen für lokale Netze (LANs) und Weitverkehrsnetze (WANs) unterstützen.

Triple DES
Ein symmetrischer Algorithmus, bei dem der unverschlüsselte Text dreimal verschlüsselt wird. Obwohl für diese Mehrfachverschlüsselung zahlreiche Methoden existieren, stellt die Triple DES-Verschlüsselung, die auf drei verschiedenen Schlüsseln basiert, das sicherste dieser Verfahren dar.

Tivoli PKI
Eine integrierte IBM Sicherheitslösung, die die Ausstellung, Erneuerung und den Widerruf digitaler Zertifikate unterstützt. Diese Zertifikate können für eine breite Palette von Internet-Anwendungen eingesetzt werden und bieten eine Möglichkeit zur Authentifizierung von Benutzern und zur Gewährleistung einer gesicherten Kommunikation.

Trust-Kette
Eine Gruppe von Zertifikaten, die aus der gesicherten Hierarchie vom Benutzerzertifikat bis zum Root- oder selbstunterzeichneten Zertifikat besteht.

Tunnel
In der VPN-Technologie eine virtuelle Punkt-zu-Punkt-Verbindung, die auf Anfrage über das Internet hergestellt wird. Während der Verbindung können ferne Benutzer den Tunnel verwenden, um sichere, verschlüsselte und gekapselte Informationen mit Servern im privaten Netz eines Unternehmens auszutauschen.

U

Unbestreitbarkeit
Die Verwendung eines digitalen, privaten Schlüssels, um zu verhindern, dass der Unterzeichner eines Dokuments dessen Unterzeichnung leugnet.

Unicode
Ein 16-Bit-Zeichensatz, der in ISO 10646 definiert ist. Der Unicodestandard für die Verschlüsselung von Zeichen ist ein internationaler Zeichencode für die Informationsverarbeitung. Er umfasst die grundlegenden, weltweit verwendeten Prozeduren und bildet die Basis für die Internationalisierung und Lokalisierung von Software. Der gesamte Quellencode in der Java-Programmierungsumgebung wird in Unicode geschrieben.

Unternehmensprozessobjekte
Eine Codegruppe, die zur Ausführung einer bestimmten Registrierungsoperation, z. B. zum Prüfen des Registrierungsstatus oder zur Bestätigung des Sendens eines öffentlichen Schlüssels, verwendet wird.

Unternehmensprozessschablone
Eine Gruppe von Unternehmensprozessobjekten, die in einer bestimmten Reihenfolge ausgeführt werden.

Unterstützung in der Landessprache (NLS)
Unterstützung für unterschiedliche länderspezifische Angaben in einem Produkt. Hierzu gehören die Sprache, die Währung, das Datums- und Zeitformat und die Darstellung von Zahlen.

Unterzeichnen
Die Verwendung eines digitalen privaten Schlüssels zum Generieren einer Unterschrift. Diese Unterschrift dient dazu, zu beweisen, dass ein bestimmter Benutzer für die von ihm unterzeichnete Nachricht verantwortlich ist und diese akzeptiert.

Unterzeichnen/Prüfen
Als Unterzeichnen wird die Verwendung eines privaten Schlüssels zum Generieren einer Unterschrift bezeichnet. Unter Prüfen versteht man die Verwendung des entsprechenden öffentlichen Schlüssels zur Verifizierung dieser Unterschrift.

Unverschlüsselter Text
Nicht verschlüsselte Daten. *Synonym zu* Klartext.

URL
Uniform Resource Locator - URL-Adresse.

URL-Adresse
Ein Schema für die Adressierung von Ressourcen im Internet. Die URL-Adresse gibt das verwendete Protokoll sowie den Host-Namen und die IP-Adresse an. Außerdem enthält er Angaben zur Anschlussnummer, zum Pfad sowie weitere Ressourcendetails, die erforderlich sind, um über eine bestimmte Maschine auf eine Ressource zuzugreifen.

UTF-8
Ein Umsetzungsformat. Es ermöglicht Informationsverarbeitungssystemen, die nur die Verarbeitung von 8-Bit-Zeichensätzen unterstützen, die Umsetzung von 16-Bit-Unicode in ein 8-Bit-Äquivalent und umgekehrt, ohne dass hierbei Informationen verloren gehen.

V

Verkettungsprüfung
Die Gültigkeitsprüfung aller CA-Unterschriften in der Trust-Hierarchie, über die ein bestimmtes Zertifikat ausgestellt wurde. Wenn z. B. das Unterschriftszertifikat eines CA über einen anderen CA ausgestellt wurde, werden bei der Gültigkeitsprüfung des vom Benutzer vorgelegten Zertifikats beide Unterschriften geprüft.

Verschlüsseln
Das Umordnen von Informationen, so dass nur Personen, die über den richtigen Entschlüsselungscode verfügen, die ursprünglichen Informationen durch Entschlüsselung abrufen können.

Verschlüsselt
Die Eigenschaft von Daten, die nach einem bestimmten System umgesetzt wurden, um deren Bedeutung unkenntlich zu machen.

Verschlüsselung/Entschlüsselung
Die Verwendung des öffentlichen Schlüssels des gewünschten Empfängers zum Verschlüsseln von Daten für diese Person. Der Empfänger verwendet anschließend den privaten Schlüssel seines Schlüsselpaares, um die Daten zu entschlüsseln.

Vertrauensdomäne
Eine Gruppe von Entitäten, deren Zertifikate vom gleichen CA zertifiziert wurden.

Vertraulichkeit
Der Schutz von Daten gegen den Zugriff nicht berechtigter Personen.

Vertraulichkeit
Die Wahrung der Geheimhaltung bestimmter Informationen gegenüber nicht berechtigten Personen.

Virtual Private Network (VPN)
Ein privates Datennetz, das ferne Verbindungen nicht über Telefonleitungen, sondern über das Internet herstellt. Da der Zugriff der Benutzer auf die Netzressourcen eines Unternehmens nicht über eine Telefongesellschaft, sondern über einen Internet Service Provider (ISP) erfolgt, können diese durch den Einsatz von VPN deutliche Einsparungen bei Fernzugriffen erzielen. Ein VPN erhöht auch die Sicherheit beim Datenaustausch. Bei der herkömmlichen Firewall-Technologie kann zwar der Inhalt der Nachricht verschlüsselt werden, nicht jedoch die Quellen- und Zieladressen. Bei der VPN-Technologie können die Benutzer eine Tunnelverbindung herstellen, bei der das gesamte Datenpaket (Header- und Datenkomponente) verschlüsselt und gekapselt ist.

Vorabregistrierung
Bei Tivoli PKI ein Prozess, mit dem ein bestimmter Benutzer (normalerweise ein Administrator) andere Benutzer registrieren kann. Wenn die Anforderung genehmigt wird, stellt die RA Informationen zur Verfügung, mit denen der Benutzer später mit Hilfe der Client-Anwendung von Tivoli PKI ein Zertifikat erhalten kann.

VPN
Virtual Private Network.

W

Web-Browser
Auf einem PC ausgeführte Client-Software, mit der ein Benutzer im World Wide Web navigieren oder lokale HTML-Seiten anzeigen kann. Der Web-Browser ist ein Abfrage-Tool, das universellen Zugriff auf die umfangreichen Hypermedia-Datensammlungen ermöglicht, die im Web und im Internet zur Verfügung gestellt werden. Manche Browser können Text und Grafik anzeigen, während andere Browser auf die Textanzeige beschränkt sind. Die meisten Browser unterstützen die Hauptformen der Internet-Kommunikation, z. B. die Ausführung von FTP-Transaktionen.

Web-Server
Ein Server-Programm, das auf Anforderungen von Browser-Programmen nach Informationsressourcen antwortet. *Siehe auch* Server.

WebSphere Application Server
Ein IBM Produkt, das Benutzer bei der Entwicklung und Verwaltung von Websites mit einem hohen Leistungsumfang unterstützt. Es erleichtert den Übergang vom einfachen Web Publishing zu komplexen e-business-Anwendungen im Web. Der WebSphere Application Server besteht aus einer Java-Servlet-Maschine, die unabhängig vom Webserver und dem verwendeten Betriebssystem arbeitet.

World Wide Web (WWW)
Der Teil des Internets, in dem ein Netz von Verbindungen zwischen Computern aufgebaut wird, auf denen Hypermediamaterial gespeichert ist. Dieses Material stellt neben Informationen auch Verbindungen (Hyperlinks) zu anderem Material im World Wide Web und Internet zur Verfügung. Der Zugriff auf WWW-Ressourcen erfolgt über einen Web-Browser.

X

X.500
Ein Standard für die Implementierung eines multifunktionalen, verteilten und vervielfältigten Verzeichnisservices durch die Verbindung von Computersystemen. Dieser Standard wurde gemeinsam definiert von der bisher als CCITT bekannten International Telecommunications Union (ITU) sowie der International Organization for Standardization und der International Electro-Chemical Commission (ISO/IEC).

X.509 Version 3-Zertifikat
Das X.509v3-Zertifikat verfügt über erweiterte Datenstrukturen für die Speicherung und das Abrufen von Informationen zu Zertifikatsanträgen, zur Zertifikatsverteilung und zu Zertifikatswiderrufen sowie zu Sicherheitsregeln und digitalen Unterschriften.
X.509v3-Prozesse dienen zum Erstellen von CRLs mit Zeitmarken für alle Zertifikate. Bei jeder Verwendung eines Zertifikats ermöglichen die X.509v3-Funktionen der Anwendung, die Gültigkeit des Zertifikats zu überprüfen. Die Anwendung kann außerdem feststellen, ob sich das Zertifikat auf der Zertifikatswiderrufsliste (CRL) befindet. CRLs unter X.509v3 können für eine bestimmte Gültigkeitsperiode erstellt werden. Sie können auch auf

anderen Kriterien basieren, die zur Aufhebung der Gültigkeit eines Zertifikats führen. Wenn z. B. ein Mitarbeiter ein Unternehmen verlässt, wird sein Zertifikat in der CRL eingetragen.

X.509-Zertifikat

Ein weit verbreiteter Zertifikatsstandard, der entwickelt wurde, um die sichere Verwaltung und Verteilung von digital unterzeichneten Zertifikaten über sichere Internet-Netze zu unterstützen. Das X.509-Zertifikat definiert Datenstrukturen, die Prozeduren für die Verteilung öffentlicher Schlüssel unterstützen, die von zuverlässigen Stellen digital unterzeichnet sind.

Z

Zertifikatsaussteller (CA)

Die Software, die zur Einhaltung der Sicherheitsregeln eines Unternehmens und zur Vergabe gesicherter elektronischer Identitäten in Form von Zertifikaten dient. Der CA verarbeitet die Anforderungen von RAs zum Ausstellen, Erneuern und Widerrufen von Zertifikaten. Er kooperiert mit der RA, um Zertifikate und CRLs im Directory zu publizieren. *Siehe auch* Digitales Zertifikat.

Zertifikatserweiterung

Eine Zusatzfunktion des X.509v3-Zertifikatformats, die zur Einbindung zusätzlicher Felder in das Zertifikat dient. Es stehen Standard- und benutzerdefinierte Erweiterungen zur Verfügung. Die Standarderweiterungen dienen verschiedenen Zwecken und umfassen Schlüssel- und Regelinformationen, Betreff- und Ausstellerattribute sowie Einschränkungen, die für den Zertifizierungspfad gelten.

Zertifikatsprofil

Eine Gruppe von Kenndaten, die den gewünschten Zertifikatstyp definieren (z. B. SSL- oder IPSec-Zertifikate). Das Profil vereinfacht die Zertifikatsspezifikation und -registrierung. Der Aussteller kann die Namen der Profile ändern und Kenndaten des gewünschten Zertifikats angeben. Hierzu zählen z. B. der Gültigkeitszeitraum, die Verwendung von Schlüsseln, DN-Einschränkungen usw.

Zertifikatsregel

Eine benannte Gruppe mit Regeln, die angibt, ob ein Zertifikat für eine bestimmte Klasse von Anwendungen mit gemeinsamen Sicherheitsanforderungen anwendbar ist. Eine Zertifikatsregel kann z. B. angeben, ob ein bestimmter Zertifizierungstyp dem Benutzer die Ausführung von Transaktionen für Waren innerhalb eines bestimmten Preisbereichs ermöglicht.

Zertifikatswiderrufsliste (CRL)

Eine digital unterzeichnete, mit Zeitmarken versehene Liste der Zertifikate, die vom Zertifikatsaussteller (CA) widerrufen wurden. Die Zertifikate in dieser Liste sollten als nicht akzeptierbar behandelt werden. *Siehe auch* Digitales Zertifikat.

Zertifizierung

Der Prozess, bei dem eine zuverlässige, an der Kommunikation nicht beteiligte Stelle (der Zertifikatsaussteller - CA) einen elektronischen Identitätsnachweis ausstellt, der für die Identität einer Person, eines Unternehmens oder einer Organisation bürgt.

Ziel

Eine benannte oder ausgewählte Datenquelle.

Zugriffssteuerungsliste (ACL)

Ein Verfahren, mit dem die Verwendung einer bestimmten Ressource auf berechtigte Benutzer beschränkt werden kann.

Index

Numerische Stichwörter

4758-CA-Profil 6
4758-RA-Profil 6

A

add_rauser (Dienstprogramm) 115
Administrator, ersten Administrator für RA hinzufügen 36
AIX
  sichern 10
  wiederherstellen 10
Aktivitätsbericht (Activity Report) 12
Aktualisieren des CA-Schlüssels 30
Aliasing, IP 80
Allgemeine Erweiterungen 69
Alternativname des Ausstellers, Erweiterung 67
Ändern von Konfigurationsdateien 9
Anforderungsdatei für Massenzertifikat 118
ASN.1 81
AuditArchiveAndSign (Dienstprogramm) 116
AuditClient.ini 84, 109
AuditIntegrityCheck (Dienstprogramm) 116
AuditServer.ini 84, 105
Authentifizierung 1

B

bciin (Befehl) 121
bcipost (Befehl) 122
bcireport (Befehl) 122
bcirunstart (Befehl) 121
bcistart (Befehl) 123
Befehle eingeben 5
Befehlszeilendienstprogramme
  Audit Archive and Sign 55
  Audit Integrity Check 55
  Bulk Certificate Issuance 118
  CA Certification 22, 25, 28, 112
  Create New RA 45, 117
  Enable RA Database Encryption 115
  Multiple RA Enrollment Authorization 118
  Multiple RA Enrollment Registration 44
  RA User 115
Berichte
  Aktivität 12
  Nutzung 11
Berichte, Prüfung 54
Bibliothek, Website von Tivoli PKI xi
Binden 51
Bulk Certificate Issuance (Dienstprogramm) 118

C

CA (Zertifikatsaussteller)
  gegenseitige Zertifizierung 66
  Hierarchien 66
    abwärts 66
    aufwärts 66
    intern 66
    unterstützte Protokolle 66
CA-Hierarchie einrichten 29
CA-Schlüssel aktualisieren 30, 124
CA-Server
  CRL-Einstellungen ändern 19
  Datenbankintegrität prüfen 21
  Konfigurationsdatei 85
  Listener-Port 18
  Protokolle 34
  Sendeaufrufintervall ändern 18
  Status 34
  verwalten 17
  Webserverzertifikat aktualisieren 30
CA-Zertifikate
  von Fremd-CA erhalten 28
CACertRq (Befehl) 25
CACertRq (Dienstprogramm) 112
CAIntegrityCheck (Dienstprogramm) 21
cakeyroll (Befehl) 30, 124
CARemac (Dienstprogramm) 20
CCITT 81
Change Password (Dienstprogramm) 5
Chiffrierschlüssel 72
createNewRA (Dienstprogramm) 117
CRL, Erstellungsintervall 19
CRL, Gültigkeitsdauer 19
CRL (Zertifikatswiderrufsliste) 70
  Einstellungen, ändern 19
  Erstellungsintervall 19
  Gültigkeitsdauer 19
CRL-Verteilungspunkte, Erweiterung 67
CRL-Verteilungspunkte aktivieren 35

D

Datei für Massenzertifikatsanforderung erstellen 118
Dateien, Konfiguration 83
Daten, Prüfdatenbank 129
Datenbankdaten, Prüfung 129
DB2-Datenbanken 79
  Protokolle 62
  Status 60
  verwalten 60
DES 64

Dienstprogramme
Add RA User 37
Aktivitätsbericht (Activity Report) 12
Audit Archive and Sign 55, 116
Audit Integrity Check 55, 116
Bulk Certificate Issuance 118
CA Certification 22, 25, 28, 112, 115
CAIntegrityCheck 21
CARemac 20
Change Password 5
Create New RA 45, 117
Enable RA Database Encryption 115
Multiple RA Enrollment Authorization 118
Multiple RA Enrollment Registration 44
Nutzungsbericht (Usage Report) 11
Trust Authority Control 7
Digitale Zertifikate 71
Digitale Zertifizierung 1
Directory 62
Directory-Administratorkennwort 6
Directory-Attribute des Zertifikatsgegenstands, Erweiterung 67
Directory-Server
Einträge 24, 28
Informationen 81
Protokolle 64
RA-Einstellungen ändern 43
Server 43
Status 63
verwalten 62
DNS-Adressen 23, 26
Domänen, Registrierung 73

E

E-Mail-Adressen 24, 27
Ereignisprotokoll 52
Ereignisse, Prüfung 49, 126
Ereignisse für Prüfadministratoren 78
Ersten Registrator hinzufügen 36
Erweiterungen
allgemein 69
Anforderungsablauf 70
Namenseinschränkungen 28
privat 69
Standard 67
Zertifikat 67

F

Fehlerbehebung 135
Fehlerprotokoll 54
Felder, Prüfereignisse 125

G

Gegenseitige Zertifizierung 22, 66, 70
Gesicherte Kommunikation 1
Gesichertes Modell, Hierarchie 25
Grundlegende Einschränkungen, Erweiterung 67
Gültigkeitsprüfung, Unterschrift 72

H

Hardwaresicherheitsmodul (HSM) 64, 73
Hierarchie
Aktualisierungen nach Änderung der CA-Hierarchie vornehmen 29
Hierarchie, CA-Zertifikat 25
Hierarchien, CA 66
Hinzufügen von Registratoren 36
Host-Name 43, 49
HSM (Hardwaresicherheitsmodul) 73
HTTP Server 15
Protokoll prüfen 17
Status 16
verwalten 15

I

iauEnableRADBSec (Dienstprogramm) 115
IBM 4758 Cryptographic Coprocessor
Aufgabenbereiche und Profile 76
Cryptographic Coprocessor 73
klonen 10, 77
Manipulationsereignisse 75
Option für Beibehaltung 74
Option für Nicht-Beibehaltung 74
verwalten 64
IBM HTTP Server 15, 80
IBM SecureWay 4758 PCI Cryptographic Coprocessor 64, 73
ICL (Issued Certificate List) 71
Schutzregel 20
Schutzschlüssel 20
Informationen zu diesem Handbuch xi
Informationszugriff für Aussteller, Erweiterung 67
Integrität 72
Integritätsprüfung 21, 55, 79
Integritätsversiegelung 79
IP-Adressen ändern 9
IP-Adressmaske 23, 26
IP-Aliasing 80
ISO 81
ITU-Standard 67, 81

J

jonahca.ini 84, 85
jonahra.ini 84, 95

K

Kennwort für Steuerprogramm 6
Kennwörter
  4758-CA-Profil 6
  4758-RA-Profil 6
  ändern 5
  Directory-Administrator 6
  Prüfadministrator 6
  Steuerprogramm 6
Kette, Trust- 73
Klonen des IBM SecureWay 4758 PCI Cryptographic Coprocessor 10
Kommunikation, gesicherte 1
Komponenten von Tivoli PKI
  CA-Server 17
  IBM Directory 62
  IBM HTTP Server 15
  IBM SecureWay 4758 PCI Cryptographic Coprocessor 64
  Prüf-Server 46
  RA-Server 35
  Server starten 7
  Server stoppen 7
  WebSphere Application Server 14
Konfigurationsdatei
  AuditClient.ini 109
  AuditServer.ini 105
  CA-Server 85
  jonahca.ini 85
  jonahra.ini 95
  Prüf-Client 109
  Prüf-Server 105
  RA-Server 95
Konfigurationsdateien 83, 84
Konventionen xiii
Kundenunterstützung xiii

L

LDAP (Lightweight Directory Access Protocol) 62
LDAP-Schemaversion angeben 103
Liste der ausgestellten Zertifikate (ICL) 71
Listener-Port 40

M

MAC-Schlüssel 72
Manipulationserkennung 78
Massenzertifikate ausstellen 118
Mehrere RAs
  Dienstprogramm Create New RA 45, 117
  Dienstprogramm Multiple RA Enrollment Authorization 118
  Dienstprogramm Multiple RA Enrollment Registration 44
  Installation 44
  Übersicht 73
Mehrere Zertifikate erstellen 118

N

Nachrichten, PKIX 65
Nachrichtenauthentifizierungscode (MAC) 66
Name des Zertifikatsgegenstands, Erweiterung 67
Namenseinschränkungen, Erweiterung 28, 67
Nutzungsbericht (Usage Report) 11
Nutzungszeitraum für privaten Schlüssel, Erweiterung 67

O

Objektkennungen (OID) 81

P

PKIX-Nachrichten 65
Port 43, 49, 51
  CA-Server 18
  Directory-Server 43
  Prüf-Server 49, 51
  RA-Server 40
Private Erweiterungen 69
Protokolle
  CA-Server 34
  DB2 62
  Directory-Server 64
  Ereignis 52
  Fehler 54
  HTTP Server 17
  Prüf-Server 59
  Prüfsubsystem 55
  Prüfung 52
  RA-Server 41
  Trace 53
  WebSphere Application Server 15
Prüfadministratorkennwort 6
Prüfen des HTTP Server-Protokolls 17
Prüfereignis 126
  Ereignisse für Prüfadministratoren 78
  Masken 78
  optional 78
  RA 78
  Schlüsselverwaltung 78
  sicherheitsrelevant 78
  verbindlich 78
  Zertifikatsverwaltung 78
Prüfmaske 49
Prüfprotokolltabelle 132
Prüfsubsystem
  Client-Konfigurationsdatei 109
  Datenbanksichten 47
  Dienstprogramm Audit Archive and Sign 116
  Dienstprogramm Audit Integrity Check 116
  Ereignismasken 78
  Fehlerprotokolleinstellungen ändern 54
  Host-Name ändern 50
  Informationen 77

Prüfsubsystem *(Forts.)*
Informationen zu Datensätzen 78
Informationen zu Ereignissen 78
Intervall zwischen Wiederholungsversuchen ändern 50
optionale Ereignisse 78
Port ändern 51
Protokolldateien archivieren 55
Protokolldateien unterzeichnen 55
Protokolle 52, 59
Protokolleinstellungen ändern 52
Prüfmaske ändern 49
Prüfprotokolleinstellungen ändern 52
Server-Konfigurationsdatei 105
Status 58
Trace-Protokolleinstellungen ändern 53
verbindliche Ereignisse 78
verwalten 46
Prüfung
Berichte generieren 54
Bindungsversuche ändern 51
Datenbankdaten 129
Host-Name ändern 49
Intervall zwischen Bindungsversuchen ändern 51
Intervall zwischen Wiederholungsversuchen ändern 50
Maske 49
Port ändern 49, 50
Protokoll 52
Protokolleinträge suchen 49
Prüfereignisse, Felder 125

Q

Quellentabelle 131

R

RA (Registrierungsstelle)
Administrator hinzufügen 37
Administratoren (Registratoren) 72
Dienstprogramm Add RA User 37, 115
ersten Administrator hinzufügen 36
ersten Registrator hinzufügen 36
Informationen 72
mehrere 73
RA-Ereignisse 78
RA-Server 35
Datenbankverschlüsselung aktivieren 39, 115
Host-Name des Directory ändern 43
Konfigurationsdatei 95
Listener-Port ändern 40
Port des Directory ändern 43
Protokolle 41
Sendeaufrufintervall ändern 40
Status 41
verwalten 35
Wiederholungsintervall ändern 41
Regeleinschränkungen, Erweiterung 67
Regelzuordnung, Erweiterung 67
Registratoren hinzufügen 36
Registrierter Name (DN) 71
Registrierungsdomänen 73
RFC 2459 67
Rollover-Prozess für CA-Schlüssel 30, 124
RSA 64

S

Schemaversion von LDAP 103
Schlüssel
MAC 72
Verschlüsselung 72
Schlüssel für CA aktualisieren 30, 124
Schlüssel-Rollover-Prozess für CA 124
Schlüsselbund des Webservers aktualisieren 29
Schlüsselkennung des Ausstellers, Erweiterung 67
Schlüsselkennung des Zertifikatsgegenstands, Erweiterung 67
Schlüsseltabelle 129
Schlüsselverwaltungsereignisse 78
Schlüsselverwendung, Erweiterung 67
Schutz
ICL-Regel 20
ICL-Schlüssel 20
Schutzregel, ICL 20
Sendeaufrufintervall 18, 40
Sendeintervall 43
Server
CA-Server 17
Directory 43, 81
HTTP 15, 80
Komponenten starten 7
Komponenten stoppen 7
Prüfung 46
RA 35
Web 79
WebSphere Application 14, 80
Sicherheit bei Tivoli PKI 65
Sicherheitsmodul für Hardware 73
Sicherheitsrelevante Ereignisse 78
Sicherung 10
AIX 10
Tivoli PKI-Datenbanken 10
Windows NT 10
Sichten der Prüfdatenbank 47
SQL-Befehl 37
Standarderweiterungen 67
Standards
ASN.1 81
CCITT 81
ISO 81
ITU 67, 81
RFC 2459 67
X.509v3 67
X.680 81
Starten von Server-Komponenten 7
Status
CA-Server 34

Status *(Forts.)*
DB2-Datenbanken 60
Directory-Server 63
HTTP Server 16
Prüf-Server 58
RA-Server 41
WebSphere Application Server 14
Stoppen von Server-Komponenten 7
Systemtabelle 134

T

Tabelle der Arten betroffener Entitäten 132
Tabelle der berechtigten Aufgabenbereiche 131
Tabelle der berechtigten Entitäten 131
Tabelle der Komponentenarten 132
Tabelle für Ereignisbewertung 130
Tabelle zur Ereignissteuerung 130
Tabellen der Prüfdatenbank
Arten betroffener Entitäten 132
berechtigte Aufgabenbereiche 131
berechtigte Entitäten 131
Ereignisbewertung 130
Ereignissteuerung 130
Komponentenarten 132
Prüfprotokoll 132
Quellen 131
Schlüssel 129
System 134
Timer 50
Tivoli
Customer Support (Kundenunterstützung) xiii
Informationen im Web zur Sicherheitsverwaltung xiii
Websites für Sicherheitsprodukte xiii
Tivoli PKI
Berichte 11, 12
Beschreibung 1
Informationen im Web xiii
IP-Adressen ändern 9
Sicherheit 65
sichern 10
Steuerung 7
verwalten 5
wiederherstellen 10
Trace-Protokoll 53

U

Übergabe der Trust-Kette
aktivieren 43
inaktivieren 43
Übersicht 73
Uniform Resource Identifiers (URIs) 24
Unterschrift, Gültigkeitsprüfung 72
Unterstützung für Tivoli Kunden xiii
Unterzeichnen 72
URIs 27
URLs
Homepage zu Tivoli PKI xi

V

Veröffentlichungen
Beschreibungen xi
Tivoli Sicherheitsprodukte xiii
Verschlüsselung für RA-Datenbank aktivieren 39
Verschlüsselungssteuerkomponente 65
Verteilungspunkte für CRL aktivieren 35
Vertraulichkeit 72
Verwalten
CA-Server 17
DB2 UDB 60
Directory-Server 62
HTTP Server 15
IBM SecureWay 4758 PCI Cryptographic Coprocessor 64
Prüfsubsystem 46
RA-Server 35
Trust Authority 5
WebSphere Application Server 14
Vorwort xi

W

Web-Server 79
Webserver aktualisieren 29
Website für
Informationen zur Sicherheitsverwaltung xiii
Tivoli Customer Support (Kundenunterstützung) xiii
Tivoli Public Key Infrastructure xiii
Tivoli Sicherheitsprodukte xiii
WebSphere Application Server 14, 80
Protokolle 15
Status 14
verwalten 14
Widerrufsliste (CRL) für Zertifikate 1
Wiederherstellen 10
AIX 10
Tivoli PKI-Datenbanken 10
Windows NT 10
Wiederholungen 50
Wiederholungsintervall 41
Windows NT
sichern 10
wiederherstellen 10

X

X.509v3 67
X.680 81

Z

Zertifikat
  Aktivität überwachen 12
  ausstellen 1
  Erneuerung 1
  Erweiterungen 67
  Nutzung überwachen 11
  widerrufen 1
  Zertifikatswiderrufsliste (CRL) 1, 70
Zertifikate 71
Zertifikate, Massenzertifikate erstellen 118
Zertifikatsaussteller (CA) 65
Zertifikatsverwaltungsereignisse 78
Zertifizierung, digitale 1, 71
Zertifizierungsregeln, Erweiterung 67
Zielgruppe xi
Zugriffssteuerungsliste (ACL) 65, 66
Zusammenfassung
  verwendete Konventionen xiii

SH12-2979-02